数 论 教 程

J.-P. 塞尔 著

冯克勤 译

丁石孙 校

上海科学技术出版社

A Course in Arithmetic

J.- P. Serre

Springer-Verlag New York Inc. 1973.

数 论 教 程

J.- P. 塞尔 著

冯 克 勤 译

丁 石 孙 校

上海科学技术出版社出版

(上海瑞金二路 450 号)

新华书店上海发行所发行 上海市印刷四厂印刷

开本 787×1092 1/32 印张 5.125 字数 110,000

1980 年 11 月第 1 版 1980 年 11 月第 1 次印刷

印数 1—6,500

书号: 13119·873 定价: (科四) 0.50 元

前　言

本书分两部分.

第一部分是纯代数的. 它的目标是有理数域上二次型的分类(Hasse-Minkowski 定理), 这工作在第四章完成. 前三章叙述某些预备知识: 二次互反律, p-adic 域, Hilbert 符号. 第五章是将上述结果用于判别式为 ±1 的整二次型. 这种二次型出现在模函数、微分拓扑和有限群等各种问题中.

第二部分(第六章和第七章)采用"解析"方法(全纯函数). 第六章给出 Dirichlet "算术级数中的素数定理"的证明; 在前一部分(第三章 §2.2)的一个关键地方曾经用过这一定理. 第七章处理模形式, 特别是 Theta 函数. 这里再次出现第五章中的某些二次型.

这两部分的材料来源于 1962 年和 1964 年国立高等学校(Ecole Normale Supérieure)大学二年级讲义. J.-J. Sansuo (第一到四章) 和 J.-P. Ramis 与 G. Ruget(第六、七章)将这些讲义作了修订, 写成了笔记. 这些笔记对我是很有益处的, 在这里我谨向这些笔记的作者表示谢意.

J.-P. 塞尔

目　录

第二部分　解 析 方 法

第 一 部 分

代 数 方 法

第一章 有 限 域

下面所考虑的域全是可交换的.

§1. 一 般 结 果

1.1. 有限域

设 K 是一个域, $\mathbf{Z}$ 在 K 中的象是一个整环, 从而同构于 $\mathbf{Z}$ 或者 $\mathbf{Z}/p\mathbf{Z}$, 其中 p 为素数; 它的商域同构于 $\mathbf{Q}$ 或者

$$\mathbf{Z}/p\mathbf{Z}=\mathbf{F}_p.$$

在第一种情形下, 称 K 为特征零域; 在第二种情形下, 称 K 为特征 p 域.

K 的特征记成 $\mathrm{char}(K)$. 如果 $\mathrm{char}(K)=p\neq 0$, 那末 p 也是满足 $n\cdot 1=0$ 的最小正整数 n.

引理 如果 $\mathrm{char}(K)=p$, 则映射 $\sigma: x\mapsto x^p$ 是 K 到其子域 K^p 上的同构.

证 我们有 $\sigma(xy)=\sigma(x)\sigma(y)$. 进而, 如果 $0<k<p$, 则二项式系数 $\binom{p}{k}\equiv 0 \pmod p$. 由此得到

$$\sigma(x+y)=\sigma(x)+\sigma(y);$$

从而 σ 是一个同态. 此外, σ 显然是单射.

定理 1 i) 有限域 K 的特征是素数 $p\neq 0$. 如果

$$f=[K:\mathbf{F}_p],$$

则 K 的元素个数为 $q=p^f$.

ii) 设 p 为素数, 且 $q=p^f (f\geqslant 1)$ 为 p 的方幂. 令 Ω 为特

征 p 的代数封闭域. 则 Ω 存在唯一的 q 元子域 $\mathbf{F}_q$, 它就是多项式 X^q-X 的根所构成的集合.

iii) 每个 $q=p^f$ 元有限域均同构于 $\mathbf{F}_q$.

证 如果 K 是有限的, 它不能包含域 $\mathbf{Q}$, 从而它的特征是素数 p. 如果 f 为扩张 $K/\mathbf{F}_p$ 的次数, 显然 $\mathrm{Card}(K)=p^f$, 这就得到 i).

另一方面, 如果 Ω 是特征 p 的代数封闭域, 上面的引理表明映射 $x\mapsto x^q$ $(q=p^f,\ f\geqslant 1)$ 是 Ω 的自同构, 这是因为此映射是自同构 σ: $x\mapsto x^p$ 重复 f 次(注意由于 Ω 代数封闭, 从而 σ 是映上). 因此对于 $x\mapsto x^q$ 不变的元素 $x\in\Omega$ 形成 Ω 的一个子域 $\mathbf{F}_q$. 多项式 X^q-X 的微商是

$$qX^{q-1}-1=p\cdot p^{f-1}X^{q-1}-1=-1,$$

即不为零. 由于 Ω 代数封闭, 这导致 X^q-X 有 q 个不同的根, 于是 $\mathrm{Card}(\mathbf{F}_q)=q$. 反之, 如果 K 是 Ω 的 q 元子域, 则 K 内非零元素组成的乘法群 K^* 有 $q-1$ 个元素. 于是若 $x\in K^*$, 则 $x^{q-1}=1$; 若 $x\in K$, 则 $x^q=x$. 这表明 K 包含在 $\mathbf{F}_q$ 之中. 由于 $\mathrm{Card}(K)=\mathrm{Card}(\mathbf{F}_q)$, 我们有 $K=\mathbf{F}_q$, 这就完成了 ii) 的证明.

由 ii) 及每个 p^f 元域均可嵌到 Ω 中 (因为 Ω 代数封闭) 这一事实即可得到 iii).

1.2. 有限域的乘法群

设 p 为素数, f 为 $\geqslant 1$ 的整数, $q=p^f$.

定理 2 有限域 $\mathbf{F}_q$ 的乘法群 $\mathbf{F}_q^*$ 是 $q-1$ 阶循环群.

证 如果 $d\geqslant 1$ 为整数, 以 $\phi(d)$ 表示 Euler ϕ-函数, 即满足 $1\leqslant x\leqslant d$ 并且与 d 互素的整数 x 的个数 (换句话说, 即在 $\mathbf{Z}/d\mathbf{Z}$ 中的象为该群生成元的 x 的个数, $1\leqslant x\leqslant d$). 显然 d 阶

循环群的生成元个数为 $\phi(d)$.

引理 1 若 $n\geqslant 1$ 为整数，则 $n=\sum_{d|n}\phi(d)$ (注意符号 $d|n$ 表示 d 整除 n).

证 如果 $d|n$，令 C_d 表示 $\mathbf{Z}/n\mathbf{Z}$ 中唯一的 d 阶子群，而以 Φ_d 表示 C_d 的生成元集合. 由于 $\mathbf{Z}/n\mathbf{Z}$中每个元素均生成某个 C_d，从而群 $\mathbf{Z}/n\mathbf{Z}$ 是所有 Φ_d 的非交并集，于是我们有

$$n=\mathrm{Card}(\mathbf{Z}/n\mathbf{Z})=\sum_{d|n}\mathrm{Card}(\Phi_d)=\sum_{d|n}\phi(d).$$

引理 2 令 H 为 n 阶有限群. 假设对 n 的每个因子 d，集合 $\{x\in H\,|\,x^d=1\}$ 至多有 d 个元素. 则 H 必为循环群.

证 设 d 为 n 的因子. 如果存在 d 阶元素 $x\in H$，则由 x 生成的子群 $(x)=\{1, x, \cdots, x^{d-1}\}$ 是 d 阶循环群. 按照假设，使 $y^d=1$ 的每个元素 $y\in H$ 均属于 (x)(特别地，H 中所有 d 阶元素都是(x)的生成元)，而它们共有 $\phi(d)$ 个. 从而 H 中 d 阶元素的个数或者为零或者为 $\phi(d)$. 如果对某个 d 的值该数是零，则公式 $n=\sum_{d|n}\phi(d)$ 表明 H 中元素的个数$<n$，这与假设相矛盾. 特别地，H 中存在着 n 阶元素 x，因而 H 即为循环群(x).

将引理 2 用于 $H=\mathbf{F}_q^*$ 和 $n=q-1$ 即得定理 2，因为次数为 d 的方程 $x^d=1$ 在 $\mathbf{F}_q$ 中至多有 d 个解.

注 由上述证明可知更一般地，一个域的乘法群的每个有限子群都是循环群.

§2. 有限域上的方程

设 q 为素数 p 的方幂，而 K 为 q 元域.

2.1. 方幂和

引理 设 $u>0$ 为整数，则和式

$$S(X^u)=\sum_{x\in K}x^u=\begin{cases}-1, & \text{当 } u\geqslant 1 \text{ 且 } (q-1)\mid u \text{ 时},\\ 0, & \text{在相反情况下}.\end{cases}$$

(当 $u=0$ 时，即使 $x=0$，也都规定 $x^u=1$.)

证 如果 $u=0$, 和式中每项均为 1, 由于 K 的特征为 p, 从而 $S(X^u)=q\cdot 1=0$.

如果 $u\geqslant 1$, 并且 $(q-1)\mid u$, 则 $0^u=0$, 而当 $x\neq 0$ 时 $x^u=1$, 从而 $S(X^u)=(q-1)\cdot 1=-1$.

最后，如果 $u\geqslant 1$, 且 $(q-1)\nmid u$, 根据定理 2, K^* 是 $q-1$ 阶循环群, 从而存在 $y\in K^*$, 使 $y^u\neq 1$, 于是有

$$S(X^u)=\sum_{x\in K^*}x^u=\sum_{x\in K^*}y^u x^u=y^u S(X^u),$$

即 $(1-y^u)S(X^u)=0$, 从而推得 $S(X^u)=0$.

(**另证** 利用如下事实：如果 $d\geqslant 2$, d 与 p 互素，则 d 次单位根之和为零.)

2.2. Chevalley 定理

定理 3 (Chevalley-Warning) 设 $f_\alpha\in K[X_1, \cdots, X_n]$ 是 n 元多项式, $\sum_\alpha \deg f_\alpha<n$, 而 V 是它们在 K^n 中的公共零点集合, 我们有

$$\operatorname{Card}(V)\equiv 0 \pmod p.$$

证 令 $P=\prod_\alpha(1-f_\alpha^{q-1})$, $x\in K^n$. 如果 $x\in V$, 则所有 $f_\alpha(x)$ 均为零, 从而 $P(x)=1$; 如果 $x\notin V$, 则必有某个 $f_\alpha(x)$ 不为零, 从而 $f_\alpha(x)^{q-1}=1$, 于是 $P(x)=0$. 因而 P 是集合 V 的特征函数. 如果对每个多项式 f, 记 $S(f)=\sum_{x\in K^n}f(x)$, 我们有

$$\operatorname{Card}(V)\equiv S(P) \pmod p,$$

于是将问题归结为证明 $S(P)=0$.

现在由假设 $\sum_{\alpha}\deg f_\alpha<n$ 可知：$\deg P<n(q-1)$. 从而 P 是单项式 $X^u=X_1^{u_1}\cdots X_n^{u_n}$ 的线性组合，其中 $\sum u_i<n(q-1)$. 只需证明对于每个这样的单项式 X^u，有 $S(X^u)=0$，而这一点由引理即可推出，因为至少有一个 $u_i<q-1$.

系 1 如果 $\sum_{\alpha}\deg f_\alpha<n$，并且每个 f_α 都没有常数项，则 f_α 有非平凡的公共零点.

证 这是因为若 V 只是 $\{0\}$，则 $p\nmid\mathrm{Card}(V)$.

系 1 可以用于当 f_α 都是齐次多项式的时候. 特别有

系 2 每个至少有 3 个变数的二次型在 K 上都有非平凡零点.

(用几何的话说，就是有限域上的每个二次超曲面都有有理点.)

§3. 二次互反律

3.1. $\mathbf{F}_q$ 中平方元素

设 q 为素数 p 的方幂.

定理 4 (a) 如果 $p=2$，则 $\mathbf{F}_q$ 中每个元素都是平方元素.

(b) 如果 $p\neq2$，则 $\mathbf{F}_q^*$ 的平方元素形成 $\mathbf{F}_q^*$ 的指数为 2 的子群，这个子群是同态

$$x\mapsto x^{(q-1)/2},\quad \mathbf{F}_p^*\to\{\pm1\}$$

的核. (换句话说，我们有正合列

$$1\to\mathbf{F}_q^{*2}\to\mathbf{F}_q^*\to\{\pm1\}\to1.)$$

证 情形(a)从 $x\mapsto x^2$ 为 $\mathbf{F}_q$ 的自同构这一事实即可推出.

对于情形(b)，令 Ω 为 $\mathbf{F}_q$ 的代数闭包. 如果 $x\in\mathbf{F}_q^*$，令 $y\in\Omega$，使 $y^2=x$. 我们有

$$y^{q-1}=x^{\frac{q-1}{2}}=\pm 1 \quad (\text{因为 } x^{q-1}=1).$$

为了 x 是 $\mathbf{F}_q$ 中的平方元素，其充要条件是 $y\in\mathbf{F}_q^*$，即 $y^{q-1}=1$. 于是 $\mathbf{F}_q^{*2}$ 为 $x\mapsto x^{\frac{q-1}{2}}$ 的核. 进而，由于 $\mathbf{F}_q^*$ 是 $q-1$ 阶循环群，从而 $\mathbf{F}_q^{*2}$ 的指数是 2.

3.2. Legendre 符号(基本情形)

定义 设 $p\neq 2$ 为素数，$x\in\mathbf{F}_p^*$. x 的 Legendre 符号 $\left(\frac{x}{p}\right)$ 是整数 $x^{\frac{p-1}{2}}=\pm 1$.

为方便起见，令 $\left(\frac{0}{p}\right)=0$，从而将 $\left(\frac{x}{p}\right)$ 扩充到 $\mathbf{F}_p$ 的全部元素上. 并且对于 $x\in\mathbf{Z}$，若 x 有象元素 $x'\in\mathbf{F}_p$，则记作

$$\left(\frac{x}{p}\right)=\left(\frac{x'}{p}\right).$$

我们有 $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)=\left(\frac{xy}{p}\right)$: Legendre 符号是"特征"(见第六章 § 1). 正如定理 4 中所表明的，$\left(\frac{x}{p}\right)=1$ 等价于 $x\in\mathbf{F}_q^{*2}$. 如果 $x\in\mathbf{F}_p^*$，x 在 $\mathbf{F}_p$ 的代数闭包中有平方根 y，则

$$\left(\frac{x}{p}\right)=y^{p-1}.$$

对于 $x=1, -1, 2$，计算$\left(\frac{x}{p}\right)$:

若 n 为奇整数，令 $\varepsilon(n)$，$\omega(n)$ 为 $\mathbf{Z}/2\mathbf{Z}$ 中的元素，定义为

$$\varepsilon(n)\equiv\frac{n-1}{2}\pmod 2=\begin{cases}0, & \text{如果 } n\equiv 1 \pmod 4,\\ 1, & \text{如果 } n\equiv -1 \pmod 4,\end{cases}$$

$$\omega(n)\equiv\frac{n^2-1}{8}\pmod 2=\begin{cases}0, & \text{如果 } n\equiv \pm 1 \pmod 8,\\ 1, & \text{如果 } n\equiv \pm 5 \pmod 8.\end{cases}$$

[函数 ε 是乘法群 $(\mathbf{Z}/4\mathbf{Z})^*$ 到 $\mathbf{Z}/2\mathbf{Z}$ 上的同态；类似地 ω 是

$(\mathbf{Z}/8\mathbf{Z})^*$ 到 $\mathbf{Z}/2\mathbf{Z}$ 上的同态.]

定理 5 i) $\left(\frac{1}{p}\right)=1$; ii) $\left(\frac{-1}{p}\right)=(-1)^{\varepsilon(p)}$; iii) $\left(\frac{2}{p}\right)=(-1)^{\omega(p)}$.

证 只有最后一个公式值得证明. 令 α 为 $\mathbf{F}_p$ 之代数闭包 Ω 中的一个 8 次本原单位根. 元素 $y=\alpha+\alpha^{-1}$, 满足 $y^2=2$ (因为由 $\alpha^4=-1$ 可知 $\alpha^2+\alpha^{-2}=0$). 我们有

$$y^p=\alpha^p+\alpha^{-p}.$$

若 $p\equiv\pm1 \pmod 8$, 这导致 $y^p=y$, 因此 $\left(\frac{2}{p}\right)=y^{p-1}=1$. 如果 $p\equiv\pm5 \pmod 8$, 我们发现

$$y^p=\alpha^5+\alpha^{-5}=-(\alpha+\alpha^{-1})=-y.$$

(这又是从 $\alpha^4=-1$ 推出来的.) 由此得到 $y^{p-1}=-1$, 从而证明了 iii).

注 定理 5 可以表达成下面的方式:

-1 是 $\bmod p$ 平方数 $\Leftrightarrow p\equiv1 \pmod 4$.

2 是 $\bmod p$ 平方数 $\Leftrightarrow p\equiv\pm1 \pmod 8$.

3.3. 二次互反律

设 l 和 p 是两个不同的奇素数.

定理 6 (Gauss) $\left(\frac{l}{p}\right)=\left(\frac{p}{l}\right)(-1)^{\varepsilon(l)\varepsilon(p)}$.

证 设 Ω 为 $\mathbf{F}_p$ 的代数闭包, $w\in\Omega$ 是 l 次本原单位根. 如果 $x\in\mathbf{F}_l$, 因为 $w^l=1$, 从而元素 w^x 是可以定义的. 于是我们可以作成 Gauss 和:

$$y=\sum_{x\in\mathbf{F}_l}\left(\frac{x}{l}\right)w^x.$$

引理 1 $y^2=(-1)^{\varepsilon(l)}l$.

(记号 l 也表示 l 在域 $\mathbf{F}_p$ 中的象.)

证　我们有

$$y^2=\sum_{x,z}\left(\frac{xz}{l}\right)w^{x+z}=\sum_{u\in\mathbf{F}_l}w^u\left(\sum_{t\in\mathbf{F}_l}\left(\frac{t(u-t)}{l}\right)\right).$$

现在若 $t\neq 0$:

$$\left(\frac{t(u-t)}{l}\right)=\left(\frac{-t^2}{l}\right)\left(\frac{1-ut^{-1}}{l}\right)=(-1)^{\varepsilon(l)}\left(\frac{1-ut^{-1}}{l}\right),$$

而
$$(-1)^{\varepsilon(l)}y^2=\sum_{u\in\mathbf{F}_l}C_uw^u,$$

其中
$$C_u=\sum_{t\in\mathbf{F}_l^*}\left(\frac{1-ut^{-1}}{l}\right).$$

如果 $u=0$, $C_0=\sum_{t\in\mathbf{F}_l^*}\left(\frac{1}{l}\right)=l-1$; 否则, $s=1-ut^{-1}$ 过 $\mathbf{F}_l-\{1\}$, 从而有

$$C_u=\sum_{s\in\mathbf{F}_l}\left(\frac{s}{l}\right)-\left(\frac{1}{l}\right)=-\left(\frac{1}{l}\right)=-1,$$

这是因为在 $\mathbf{F}_l^*$ 中平方元素和非平方元素有同样多个. 于是

$$\sum_{u\in\mathbf{F}_l}C_uw^u=l-1-\sum_{u\in\mathbf{F}_l^*}w^u=l,$$

此即证明了引理.

引理 2　$y^{p-1}=\left(\frac{p}{l}\right)$.

证　由于 Ω 的特征是 p, 我们有

$$y^p=\sum_{x\in\mathbf{F}_l}\left(\frac{x}{p}\right)w^{xp}=\sum_{z\in\mathbf{F}_l}\left(\frac{zp^{-1}}{l}\right)w^z=\left(\frac{p^{-1}}{l}\right)y=\left(\frac{p}{l}\right)y,$$

从而
$$y^{p-1}=\left(\frac{p}{l}\right).$$

现在可以证明定理 6. 由引理 1 和引理 2, 有

$$\left(\frac{(-1)^{\varepsilon(l)}l}{p}\right)=y^{p-1}=\left(\frac{p}{l}\right),$$

而定理 5 的第二部分表明

$$\left(\frac{(-1)^{\varepsilon(l)}}{p}\right)=(-1)^{\varepsilon(l)\varepsilon(p)}.$$

如果把 l 是 $\bmod p$ 平方数(即 l 是 $\bmod p$"二次剩余")表示成 lRp, 否则表示成 lNp. 则定理 6 可以叙述为

$$lRp \Leftrightarrow pRl, \quad 当 p 或 l \equiv 1 \pmod 4 时;$$

$$lRp \Leftrightarrow pNl, \quad 当 p 和 l \equiv -1 \pmod 4 时.$$

注 定理 6 可使我们采用逐次化简的方法计算Legendre符号. 例如

$$\left(\frac{29}{43}\right)=\left(\frac{43}{29}\right)=\left(\frac{14}{29}\right)=\left(\frac{2}{29}\right)\left(\frac{7}{29}\right)$$

$$=-\left(\frac{7}{29}\right)=-\left(\frac{29}{7}\right)=-\left(\frac{1}{7}\right)=-1.$$

附录 二次互反律的另一证明

(G. Eisenstein, J. Crelle, 29, 1845, pp. 177～184.)

i) Gauss 引理

设 p 为奇素数, S 为 $\mathbf{F}_p^*$ 的子集, 使 $\mathbf{F}_p^*$ 为 S 和 $-S$ 的非交并集. 以下我们取 $S=\left\{1, \cdots, \frac{p-1}{2}\right\}$.

如果 $s\in S$, $a\in\mathbf{F}_p^*$, 我们记成形式

$$as=e_s(a)s_a, \quad e_s(a)=\pm 1, \quad s_a\in S.$$

引理(Gauss) $\left(\frac{a}{p}\right)=\prod_{s\in S} e_s(a)$.

证 首先注意, 如果 s 和 s' 是 S 中两个不同的元素, 则 $s_a\neq s'_a$(因为否则 $s=\pm s'$, 与 S 之选取相矛盾). 这说明 $s\mapsto s_a$ 是 S 到它本身之上的一一对应. 将诸等式 $as=e_s(a)s_a$ 相乘, 得到

$$a^{\frac{(p-1)}{2}}\prod_{s\in S}s=\Big(\prod_{s\in S}e_s(a)\Big)\prod_{s\in S}s_a=\Big(\prod_{s\in S}e_s(a)\Big)\prod_{s\in S}s,$$

于是
$$a^{\frac{p-1}{2}}=\prod_{s\in S}e_s(a),$$

因为在 $\mathbf{F}_p$ 中 $\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}}$, 这就证明了引理.

【例】 取 $a=2$, $S=\left\{1, \cdots, \frac{p-1}{2}\right\}$. 有

$$e_s(2)=\begin{cases}1, & \text{如果 } 2s\leqslant\frac{p-1}{2},\\ -1, & \text{否则.}\end{cases}$$

由此得到 $\left(\frac{2}{p}\right)=(-1)^{n(p)}$, 这里 $n(p)$ 是满足 $\frac{p-1}{4}<s\leqslant\frac{p-1}{2}$ 的整数 s 的个数. 如果 p 有形式 $1+4k$(或 $3+4k$), 则 $n(p)=k$(或 $n(p)=k+1$). 因此我们发现, 当 $p\equiv\pm1 \pmod 8$ 时, $\left(\frac{2}{p}\right)=1$; 而当 $p\equiv\pm5 \pmod 8$ 时, $\left(\frac{2}{p}\right)=-1$, 参见定理 5.

ii) 一个关于三角函数的引理

引理　设 m 为奇自然数. 则有

$$\frac{\sin mx}{\sin x}=(-4)^{\frac{m-1}{2}}\prod_{1\leqslant j\leqslant\frac{m-1}{2}}\left(\sin^2 x-\sin^2\frac{2\pi j}{m}\right).$$

证明是初等的. (例如, 可先证 $\frac{\sin mx}{\sin x}$ 是对于变量 $\sin^2 x$ 的 $\frac{m-1}{2}$ 次多项式, 然后注意这个多项式有根 $\sin^2\frac{2\pi j}{m}\left(1\leqslant j\leqslant\frac{m-1}{2}\right)$, 比较 $e^{i(m-1)x}$ 两边的系数, 即得到因子 $(-4)^{\frac{m-1}{2}}$.)

iii) 二次互反律的证明

设 l 和 p 是两个不同的奇素数. 如上一样, 令

$$S=\left\{1, \cdots, \frac{p-1}{2}\right\}.$$

从 Gauss 引理得到

$$\left(\frac{l}{p}\right)=\prod_{s\in S}e_s(l).$$

现在等式 $ls=e_s(l)s_l$ 表明

$$\sin\frac{2\pi}{p}ls=e_s(l)\sin\frac{2\pi}{p}s_l.$$

将这些等式相乘, 并考虑到 $s\mapsto s_l$ 是 S 上的一一对应, 便得到

$$\left(\frac{l}{p}\right)=\prod_{s\in S}e_s(l)=\prod_{s\in S}\sin\frac{2\pi ls}{p}\bigg/\sin\frac{2\pi s}{p}.$$

对于 $m=l$, 利用上面三角函数的引理, 可以将它重写为

$$\left(\frac{l}{p}\right)=\prod_{s\in S}(-4)^{\frac{l-1}{2}}\prod_{t\in T}\left(\sin^2\frac{2\pi s}{p}-\sin^2\frac{2\pi t}{l}\right)$$
$$=(-4)^{\frac{(l-1)(p-1)}{4}}\prod_{\substack{t\in T\\ s\in S}}\left(\sin^2\frac{2\pi s}{p}-\sin^2\frac{2\pi t}{l}\right),$$

其中 T 表示从1到 $\frac{l-1}{2}$ 的整数集合. 交换 l 和 p 的地位，可以类似地得到:

$$\left(\frac{p}{l}\right)=(-4)^{\frac{(l-1)(p-1)}{4}}\prod_{\substack{s\in S\\ t\in T}}\left(\sin^2\frac{2\pi t}{l}-\sin^2\frac{2\pi s}{p}\right).$$

$\left(\frac{l}{p}\right)$ 和 $\left(\frac{p}{l}\right)$ 的上述二分解式基本上相同，只相差 $\frac{(p-1)(l-1)}{4}$ 个符号，于是可得到

$$\left(\frac{l}{p}\right)=\left(\frac{p}{l}\right)(-1)^{\frac{(p-1)(l-1)}{4}}.$$

这就是二次互反律，见定理6.

第二章 p-adic 域

在本章中 p 表示素数.

§1. 环 $\mathbf{Z}_p$ 和域 $\mathbf{Q}_p$

1.1. 定义

对于每个 $n\geqslant 1$, 令 $A_n=\mathbf{Z}/p^n\mathbf{Z}$, 这是 $\bmod p^n$ 同余类环. A_n 中的一个元素以明显的方式决定出 A_{n-1} 中的一个元素, 由此得到同态

$$\phi_n:\ A_n\to A_{n-1},$$

它是映上的, 并且核是 $p^{n-1}A_n$.

序列 $\cdots\to A_n\to A_{n-1}\to\cdots\to A_2\to A_1$

形成以自然数为指标的"投射系".

定义 1 p-adic 整数环 $\mathbf{Z}_p$ 是上面定义的系 (A_n, ϕ_n) 的投射极限.

按照定义, $\mathbf{Z}_p=\varprojlim(A_n, \phi_n)$ 中的元素是序列 $x=(\cdots, x_n, \cdots, x_1)$, 其中 $x_n\in A_n$, 而当 $x\geqslant 2$ 时, $\phi_n(x_n)=x_{n-1}$. $\mathbf{Z}_p$ 中的加法和乘法定义成"按坐标"运算. 换句话说, $\mathbf{Z}_p$ 是积 $\prod\limits_{n\geqslant 1}A_n$ 的子环. 如果 A_n 赋以离散拓扑, 而 $\prod A_n$ 赋以积拓扑, 则环 $\mathbf{Z}_p$ 得到一个拓扑, $\mathbf{Z}_p$ 对此拓扑是紧拓扑空间(因为它在紧拓扑空间的积空间中是闭的).

1.2. $\mathbf{Z}_p$ 的性质

设 ε_n: $\mathbf{Z}_p\to A_n$ 为一函数, 它将 p-adic 整数 x 映成其第 n

个分量 x_n.

命题 1 序列 $0 \to \mathbf{Z}_p \xrightarrow{p^n} \mathbf{Z}_p \xrightarrow{\varepsilon_n} A_n \to 0$ 是 Abel 群的正合列.

(因此可以将 $\mathbf{Z}_p/p^n\mathbf{Z}_p$ 和 $A_n=\mathbf{Z}/p^n\mathbf{Z}$ 等同.)

证 乘以 p 是 $\mathbf{Z}_p$ 中的单射, 因为若 $x=(x_n)$ 是 p-adic 整数, 使得 $px=0$, 则对每个 n, 有 $px_{n+1}=0$. 于是 x_{n+1} 有形式 $p^n y_{n+1}$, $y_{n+1}\in A_{n+1}$. 因为 $x_n=\phi_{n+1}(x_{n+1})$, 从而 $p^n|x_n$, 于是 $x_n=0$. 既然乘以 p 是 $\mathbf{Z}_p$ 中的单射, 那末乘以 p^n 也是 $\mathbf{Z}_p$ 中的单射.

ε_n 的核显然包含 $p^n\mathbf{Z}_p$. 反之, 若 $x=(x_m)\in\ker(\varepsilon_n)$, 则对所有的 $m\geqslant n$, 均有 $x_m\equiv 0 \pmod{p^n}$, 这意味着存在 A_{m-n} 中一个可定义的元素 y_{m-n}, 使它在同构

$$A_{m-n}\to p^n\mathbf{Z}/p^m\mathbf{Z}\subset A_m$$

之下的象满足 $x_m=p^n y_{m-n}$. 这些 y_i 定义了 $\mathbf{Z}_p=\varprojlim A_i$ 中一元素 y, 易知有 $p^n y=x$, 这就证明了命题.

命题 2 (a) $\mathbf{Z}_p$(或 A_n)中一元素可逆的充要条件是它不能被 p 除尽.

(b) 如果以 $\mathbf{U}$ 表示 $\mathbf{Z}_p$ 中的可逆元素群, 则 $\mathbf{Z}_p$ 中每个非零元素均可唯一地写成形式 $p^n u$, 其中 $u\in\mathbf{U}$, 而 $n\geqslant 0$. ($\mathbf{U}$ 中元素称为 p-adic 单位.)

证 只需对 A_n 证明 (a), 然后立即可得到对于 $\mathbf{Z}_p$ 的情形. 现在, 如果 $x\in A_n$, x 不属于 pA_n, 则它在 $A_1=\mathbf{F}_p$ 中的象不为零, 从而是可逆的, 于是存在 y, $z\in A_n$, 使 $xy=1-pz$, 从而

$$xy(1+pz+\cdots+p^{n-1}z^{n-1})=1.$$

这就证明了 x 是可逆的.

另一方面, 如果 $x\in\mathbf{Z}_p$ 不为零, 则有一个最大的整数 n,

使 $x_n=\varepsilon_n(x)$ 为零. 于是 $x=p^n u$, $p\nmid u$, 由(a)即知 $u\in\mathbf{U}$. 分解的唯一性是显然的.

记法 设 x 为 $\mathbf{Z}_p$ 中非零元素, 把 x 写成形式 $x=p^n u$, $u\in\mathbf{U}$. 整数 n 称为 x 的 p-adic 赋值, 记成 $v_p(x)$. 规定 $v_p(0)=+\infty$, 于是有

$$v_p(xy)=v_p(x)+v_p(y),$$
$$v_p(x+y)\geqslant\inf(v_p(x),\ v_p(y)).$$

从这些公式不难推出 $\mathbf{Z}_p$ 是整环.

命题 3 $\mathbf{Z}_p$ 上的拓扑可以由距离

$$d(x,\ y)=e^{-v_p(x-y)}$$

定义, 这时环 $\mathbf{Z}_p$ 为完备度量空间, 而 $\mathbf{Z}$ 在 $\mathbf{Z}_p$ 中是稠密的.

证 理想 $p^n\mathbf{Z}_p$ 形成 0 的邻域基. 由于 $x\in p^n\mathbf{Z}_p$ 等价于 $v_p(x)\geqslant n$, 从而 $\mathbf{Z}_p$ 的拓扑可由距离 $d(x,\ y)=e^{-v_p(x-y)}$ 定义. 因为 $\mathbf{Z}_p$ 是紧致的, 从而是完备的. 最后, 如果 $x=(x_n)$ 是 $\mathbf{Z}_p$ 的元素, 并且有 $y_n\in\mathbf{Z}$, 使 $y_n\equiv x_n \pmod{p^n}$, 则 $\lim y_n=x$, 这就证明了 $\mathbf{Z}$ 在 $\mathbf{Z}_p$ 中是稠密的.

1.3. 域 $\mathbf{Q}_p$

定义 2 环 $\mathbf{Z}_p$ 的商域称为 p-adic 数域, 用 $\mathbf{Q}_p$ 表示.

由此立即得到 $\mathbf{Q}_p=\mathbf{Z}_p[p^{-1}]$. 每个元素 $x\in\mathbf{Q}_p^*$ 可以唯一地表示成形式 $p^n u$, 其中 $n\in\mathbf{Z}$, $u\in\mathbf{U}$. n 仍称作 x 的 p-adic 赋值, 记为 $v_p(x)$. 于是有 $v_p(x)\geqslant 0\Leftrightarrow x\in\mathbf{Z}_p$.

命题 4 域 $\mathbf{Q}_p$ 对于由 $d(x,\ y)=e^{-v_p(x-y)}$ 定义的拓扑是局部紧拓扑空间, $\mathbf{Z}_p$ 为 $\mathbf{Q}_p$ 的开子环, 而域 $\mathbf{Q}$ 在 $\mathbf{Q}_p$ 中是稠密的.

证明是显然的.

注 1) 可以定义 $\mathbf{Q}_p$(或 $\mathbf{Z}_p$) 为 $\mathbf{Q}$ (或 $\mathbf{Z}$) 对于 p-adic 距

离 d 的完备化.

2) 距离 d 满足"超距"不等式

$$d(x, z) \leqslant \sup(d(x, y), d(y, z)).$$

由此可知，序列 u_n 有极限 $\Leftrightarrow \lim(u_{n+1}-u_n)=0$. 类似地，一个级数收敛$\Leftrightarrow$其通项趋于零.

§2. p-adic 方 程

2.1. 解

引理 设 $\cdots \to D_n \to D_{n-1} \to \cdots \to D_1$ 是投射系，而

$$D = \varprojlim D_n$$

是它们的投射极限. 如果每个 D_n 都是有限的且为非空的，则 D 也是非空的.

证 如果 $D_n \to D_{n-1}$ 均是映上的，则显然 $D \neq \emptyset$. 现在把引理归结到这种特殊情形. 为此，以 $D_{n,p}$ 表示 D_{n+p} 在 D_n 中的象. 对于固定的 n, $D_{n,p}$ 形成一个有限非空子集的下降族，从而这个集族是稳定的，即当 p 充分大时，$D_{n,p}$ 与 p 无关. 以 E_n 表示 $D_{n,p}$ 的极限值. 不难看出 $D_n \to D_{n-1}$ 将 E_n 映到 E_{n-1} 上. 因为 E_n 是非空的，由本证明一开始所述可知:

$$\varprojlim E_n \neq \emptyset. \quad \text{于是} \quad \varprojlim D_n \neq \emptyset.$$

记法 设 $f \in \mathbf{Z}_p[X_1, \cdots, X_m]$ 为系数属于 $\mathbf{Z}_p$ 的多项式，n 是自然数，我们把 f 经 $(\bmod p^n)$ 简化而得到的系数属于 A_n 的多项式记为 f_n.

命题 5 设 $f^{(i)} \in \mathbf{Z}_p[X_1, \cdots, X_m]$ 是 p-adic 整系数多项式，则下列两条是等价的:

1) $f^{(i)}$ 在 $(\mathbf{Z}_p)^m$ 中有公共零点.

2) 对于每个 $n \geqslant 1$, 多项式 $f_n^{(i)}$ 在 $(A_n)^m$ 中有公共零点.

证 以 D(或 D_n)表示 $f^{(i)}$(或 $f_n^{(i)}$) 的公共零点集合. D_n 是有限集合, 并且 $D=\varprojlim D_n$. 根据上述引理, D 非空 $\Leftrightarrow D_n$ 均非空. 从而证明了命题.

点 $x=(x_1, \cdots, x_m)\in(\mathbf{Z}_p)^m$ 称为本原的, 是指某个 x_i 可逆, 即 x_i 不全被 p 所除尽. 类似地定义 $(A_n)^m$ 中的本原元素.

命题 6 设 $f^{(i)}\in\mathbf{Z}_p[X_1, \cdots, X_m]$ 是具有 p-adic 整系数的齐次多项式, 则下列三条彼此等价:

a) $f^{(i)}$ 在 $(\mathbf{Q}_p)^m$ 中有非平凡公共零点.

b) $f^{(i)}$ 在 $(\mathbf{Z}_p)^m$ 中有公共本原零点.

c) 对每个 $n\geqslant 1$, $f_n^{(i)}$ 在 $(A_n)^m$ 中有公共本原零点.

证 b)$\Rightarrow$a) 是显然的. 反之, 如果 $x=(x_1, \cdots, x_m)$ 是 $f^{(i)}$ 的非平凡公共零点, 令

$$h=\inf(v_p(x_1), \cdots, v_p(x_m)), \quad y=p^{-h}x.$$

显然 y 是 $(\mathbf{Z}_p)^m$ 中的本原元素, 并且它是 $f^{(i)}$ 的公共零点. 于是 a)$\Leftrightarrow$b).

b) 和 c) 的等价性可以从上述引理推出.

2.2. 近似解的改进

现在讨论如何从一个 $\bmod p^n$ 解得到一个真正的解 (即系数在 $\mathbf{Z}_p$ 中的解). 这要用下面的引理("Newton 法"的 p-adic 模拟).

引理 设 $f\in\mathbf{Z}_p[X]$, f' 为它的微商. 令 $x\in\mathbf{Z}_p$, $n, k\in\mathbf{Z}$, 使 $0\leqslant 2k<n$, $f(x)\equiv 0 \pmod{p^n}$, $v_p(f'(x))=k$. 则存在 $y\in\mathbf{Z}_p$, 使

$$f(y)\equiv 0 \pmod{p^{n+1}}, \quad v_p(f'(y))=k,$$

$$y\equiv x \pmod{p^{n-k}}.$$

证 取形如 $x+p^{n-k}z$ 的 y，其中 $z\in\mathbf{Z}_p$. 由 Taylor 公式可得

$$f(y)=f(x)+p^{n-k}zf'(x)+p^{2n-2k}a,$$

其中 $$a\in\mathbf{Z}_p.$$

根据假设，$f(x)=p^nb$, $f'(x)=p^kc$, $b\in\mathbf{Z}_p$, $c\in\mathbf{U}$. 这就可以选取 z 使

$$b+zc\equiv0\ (\mathrm{mod}\ p).$$

由此可得到

$$f(y)=p^n(b+zc)+p^{2n-2k}a\equiv0\ (\mathrm{mod}\ p^{n+1}),$$

这是因为 $2n-2k>n$. 最后，对于 f' 利用 Taylor 公式可以证得 $f'(y)\equiv p^kc\ (\mathrm{mod}\ p^{n-k})$. 因为 $n-k>k$, 于是可以看到

$$v_p(f'(y))=k.$$

定理 1 设 $f\in\mathbf{Z}_p[X_1,\ \cdots,\ X_m]$, $x=(x_i)\in(\mathbf{Z}_p)^m$, n, $k\in\mathbf{Z}$, j 为整数，满足 $1\leqslant j\leqslant m$. 又设 $0\leqslant 2k<n$, 并且

$$f(x)\equiv0\ (\mathrm{mod}\ p^n),\quad v_p\left(\frac{\partial f}{\partial X_j}(x)\right)=k.$$

则 f 在 $(\mathbf{Z}_p)^m$ 中有一个零点 y, 使 $y\equiv x\ (\mathrm{mod}\ p^{n-k})$.

证 先设 $m=1$. 将上述引理用于 $x^{(0)}=x$, 则得到 $x^{(1)}\in\mathbf{Z}_p$, $x^{(1)}\equiv x^{(0)}\ (\mathrm{mod}\ p^{n-k})$, 并且

$$f(x^{(1)})\equiv0\ (\mathrm{mod}\ p^{n+1}),\quad v_p(f'(x^{(1)}))=k.$$

用 $n+1$ 代替 n, 再对 $x^{(1)}$应用上述引理. 归纳地进行下去，这样就构造一个序列 $x^{(0)}$, $\cdots$, $x^{(q)}$, $\cdots$, 使

$$x^{(q+1)}\equiv x^{(q)}\ (\mathrm{mod}\ p^{n+q-k}),\quad f(x^{(q)})\equiv0\ (\mathrm{mod}\ p^{n+q}).$$

这是一个 Cauchy 序列. 如果 y 是它的极限，则有 $f(y)=0$, 并且 $y\equiv x\ (\mathrm{mod}\ p^{n-k})$, 从而对于 $m=1$, 定理得到了证明.

对于 $m>1$ 的情况，如果只考虑 x_j, 则归结为 $m=1$ 的情况. 更确切地说，设 $\tilde{f}\in\mathbf{Z}_p[X_j]$是一个单变量多项式，它由对所有的 $i\neq j$, 将 f 中的 X_i 代之以 x_i 而得到. 将上述所证

的事实用于 $\bar{f}$ 和 x_j，则可知存在 $y_j\equiv x_j\ (\bmod p^{n-k})$，使 $\bar{f}(y_j)=0$. 如果令 $y_i=x_i$(对于 $i\neq j$)，则元素 $y=(y_i)$ 满足所需要的条件.

系 1 $\mathbf{Z}_p$ 上多项式 f 的 $\bmod p$ 简化的每个单零点均可提升成 f 在 $\mathbf{Z}_p$ 中的一个零点.

(如果 g 是域 K 上多项式，g 的零点 x 叫作单零点，是指至少有一个偏微商 $\dfrac{\partial g}{\partial X_j}$ 在 x 处不是零.)

这是 $n=1$, $k=0$ 的特殊情形.

系 2 设 $p\neq 2$, $f(X)=\sum a_{ij}X_iX_j$ 为系数属于 $\mathbf{Z}_p$ 的二次型，$a_{ij}=a_{ji}$，并且判别式 $\det(a_{ij})$ 可逆. 令 $a\in\mathbf{Z}_p$. 则方程 $f(x)\equiv a\ (\bmod p)$ 的每个本原解均可提升成一个真正解.

证 按照系 1，我们只需证明 x 不是 f 的所有偏微商的 $\bmod p$ 零点. 现在 $\dfrac{\partial f}{\partial X_i}=2\sum_j a_{ij}X_j$. 由于 $\det(a_{ij})\not\equiv 0\ (\bmod p)$，而 x 为本原元素，从而必有一个偏微商 $\not\equiv 0\ (\bmod p)$.

系 3 设 $p=2$，令 $f=\sum a_{ij}X_iX_j$ 是系数属于 $\mathbf{Z}_2$ 的二次型，$a_{ij}=a_{ji}$，设 $a\in Z_2$. 令 x 是 $f(x)\equiv a(\bmod 8)$ 的本原解. 如果 x 不是所有 $\dfrac{\partial f}{\partial X_j}$ 的 $\bmod 4$ 零点，则我们可以把 x 提升成一个真正解. 如果 $\det(a_{ij})$ 可逆，则后一条件是满足的.

证 将定理用于情形 $n=3$, $k=1$，即可证得第一论断. 第二论断可以象 $p\neq 2$ 情形一样证得 (但要取出一个因子 2).

§3. $\mathbf{Q}_p$ 的乘法群

3.1. 单位群的滲透(filtration)

设 $\mathbf{U}=\mathbf{Z}_p^*$ 为 p-adic 单位群. 对于每个 $n\geqslant 1$，令

$$\mathbf{U}_n=1+p^n\mathbf{Z}_p.$$

这是同态 ε_n: $\mathbf{U}\to(\mathbf{Z}/p^n\mathbf{Z})^*$ 的核. 特别地, 商 $\mathbf{U}/\mathbf{U}_1$ 可以等同于 $\mathbf{F}_p^*$, 从而是 $p-1$ 阶循环群(见第一章定理 2). $\mathbf{U}_n$ 形成 $\mathbf{U}$ 之开子群下降列, 并且 $\mathbf{U}=\varprojlim \mathbf{U}/\mathbf{U}_n$. 如果 $n\geqslant 1$, 映射

$$(1+p^n x)\mapsto x \pmod p$$

定义一个同构 $\mathbf{U}_n/\mathbf{U}_{n+1}\to\mathbf{Z}/p\mathbf{Z}$, 这由公式

$$(1+p^n x)(1+p^n y)\equiv 1+p^n(x+y) \pmod{p^{n+1}}$$

便可推出. 由此对 n 归纳, 即知 $\mathbf{U}_1/\mathbf{U}_n$ 的阶是 p^{n-1}.

引理 设 $0\to A\to E\to B\to 0$ 是交换群正合列(群运算表示成加法), A 和 B 为有限群, 其阶数 a 和 b 互素. 令

$$B'=\{x\in E\mid bx=0\}.$$

则群 E 是 A 和 B' 的直和. 并且 B' 是 E 中同构于 B 的唯一子群.

证 因为 a 与 b 互素, 从而存在 r, $s\in\mathbf{Z}$, 使 $ar+bs=1$. 如果 $x\in A\cap B'$, 则 $ax=bx=0$, 于是 $x=(ar+bs)x=0$, 即 $A\cap B'=0$. 进而, 每个 $x\in E$ 均可写成 $x=arx+bsx$. 由于 $bB=0$, 于是 $bE\subset A$, 从而 $bsx\in A$. 另一方面, 由 $abE=0$ 可知 $arx\in B'$. 于是有 $E=A\oplus B'$, 并且射影 $E\to B$ 定义了 B' 到 B 上的一个同构. 反之, 如果 B'' 是 E 的子群并且同构于 B, 我们有 $bB''=0$, 于是 $B''\subset B'$, 但是此两群的阶数相同, 从而 $B''=B'$.

命题 7 我们有 $\mathbf{U}=\mathbf{V}\times\mathbf{U}_1$, 其中 $\mathbf{V}=\{x\in\mathbf{U}\mid x^{p-1}=1\}$ 是 $\mathbf{U}$ 的同构于 $\mathbf{F}_p^*$ 的唯一子群.

证 将引理用于正合列

$$1\to\mathbf{U}_1/\mathbf{U}_n\to\mathbf{U}/\mathbf{U}_n\to\mathbf{F}_p^*\to 1,$$

其合理性是因为 $\mathbf{U}_1/\mathbf{U}_n$ 的阶数为 p^{n-1} 而 $\mathbf{F}_p^*$ 的阶数为 $p-1$. 由此可知 $\mathbf{U}/\mathbf{U}_n$ 包含唯一的一个子群 $\mathbf{V}_n$ 同构于 $\mathbf{F}_q^*$, 并且射影

$$\mathbf{U}/\mathbf{U}_n \to \mathbf{U}/\mathbf{U}_{n-1}$$

将 $\mathbf{V}_n$ 同构地映到 $\mathbf{V}_{n-1}$ 上. 因为 $\mathbf{U}=\varprojlim \mathbf{U}/\mathbf{U}_n$, 由此取极限, 得到 $\mathbf{U}$ 的一个子群 $\mathbf{V}$ 同构于 $\mathbf{F}_p^*$, 并且 $\mathbf{U}=\mathbf{V}\times\mathbf{U}_1$. $\mathbf{V}$ 的唯一性从 $\mathbf{V}_n$ 的唯一性推得.

系 域 $\mathbf{Q}_p$ 包含 $(p-1)$ 次单位根.

注 1) 群 $\mathbf{V}$ 叫作 $\mathbf{F}_p^*$ 中元素的乘法表示群.

2) 还可以将定理 1 的系 1 用于方程 $x^{p-1}-1=0$ 来证明 $\mathbf{V}$ 的存在性.

3.2. 群 $\mathbf{U}_1$ 的结构

引理 设 $x\in\mathbf{U}_n-\mathbf{U}_{n+1}$, 其中当 $p\neq 2$ 时令 $n\geqslant 1$, 而 $p=2$ 时令 $n\geqslant 2$. 则 $x^p\in\mathbf{U}_{n+1}-\mathbf{U}_{n+2}$.

证 由假设我们有 $x=1+kp^n$, $k\not\equiv 0 \pmod p$. 二项式定理给出

$$x^p=1+kp^{n+1}+\cdots+k^pp^{np}.$$

而没有写出来的各项的指数均 $\geqslant 2n+1\geqslant n+2$. 而且

$$np\geqslant n+2 \quad (\text{因为当 } p=2 \text{ 时 } n\geqslant 2).$$

这就证明了

$$x^p\equiv 1+kp^{n+1} \pmod{p^{n+2}}.$$

于是
$$x^p\in\mathbf{U}_{n+1}-\mathbf{U}_{n+2}.$$

命题 8 若 $p\neq 2$, 则 $\mathbf{U}_1$ 同构于 $\mathbf{Z}_p$.

如果 $p=2$, 则 $\mathbf{U}_1=\{\pm 1\}\times\mathbf{U}_2$, 而 $\mathbf{U}_2$ 同构于 $\mathbf{Z}_2$.

证 先考虑 $p\neq 2$ 的情形. 取一元素 $\alpha\in\mathbf{U}_1-\mathbf{U}_2$, 例如令 $\alpha=1+p$. 按照上面引理我们有 $\alpha^{p^i}\in\mathbf{U}_{i+1}-\mathbf{U}_{i+2}$. 令 α_n 为 α 在 $\mathbf{U}_1/\mathbf{U}_n$ 中的象. 我们有 $(\alpha_n)^{p^{n-2}}\neq 1$, 而 $(\alpha_n)^{p^{n-1}}=1$. 但是 $\mathbf{U}_1/\mathbf{U}_n$ 的阶数为 p^{n-1}, 从而它是由 α_n 生成的循环群. 现在用 $\theta_{n,\alpha}$ 表示 $\mathbf{Z}/p^{n-1}\mathbf{Z}$ 到 $\mathbf{U}_1/\mathbf{U}_n$ 上的同构 $z\mapsto\alpha_n^z$, 便有交换图

$$\begin{array}{ccc} \mathbf{Z}/p^n\mathbf{Z} & \xrightarrow{\theta_{n+1,\alpha}} & \mathbf{U}_1/\mathbf{U}_{n+1} \\ \downarrow & & \downarrow \\ \mathbf{Z}/p^{n-1}\mathbf{Z} & \xrightarrow{\theta_{n,\alpha}} & \mathbf{U}_1/\mathbf{U}_n \end{array}$$

由此可知 $\theta_{n,\alpha}$ 决定出 $\mathbf{Z}_p=\varprojlim \mathbf{Z}/p^{n-1}\mathbf{Z}$ 到 $\mathbf{U}_1=\varprojlim \mathbf{U}_1/\mathbf{U}_n$ 上的一个同构 θ, 从而对于 $p\neq 2$ 证明了命题.

现在设 $p=2$. 取 $\alpha\in\mathbf{U}_2-\mathbf{U}_3$, 即 $\alpha\equiv 5 \pmod 8$. 类似于上面那样定义同构

$$\theta_{n,\alpha}:\ \mathbf{Z}/2^{n-2}\mathbf{Z}\to\mathbf{U}_2/\mathbf{U}_n,$$

于是有同构 θ_α: $\mathbf{Z}_2\to\mathbf{U}_2$. 另一方面, 同态

$$\mathbf{U}_1\to\mathbf{U}_1/\mathbf{U}_2\simeq\mathbf{Z}/2\mathbf{Z}$$

诱导出 $\{\pm 1\}$ 到 $\mathbf{Z}/2\mathbf{Z}$ 上的一个同构. 由此得到

$$\mathbf{U}_1=\{\pm 1\}\times\mathbf{U}_2.$$

定理 2 如果 $p\neq 2$,则群 $\mathbf{Q}_p^*$ 同构于 $\mathbf{Z}\times\mathbf{Z}_p\times\mathbf{Z}/(p-1)\mathbf{Z}$. 如果 $p=2$, 则 $\mathbf{Q}_2^*$ 同构于 $\mathbf{Z}\times\mathbf{Z}_2\times\mathbf{Z}/2\mathbf{Z}$.

证 每个元素 $x\in\mathbf{Q}_p^*$ 可以唯一地写成形式 $x=p^n u$, 其中 $n\in\mathbf{Z}$, $u\in\mathbf{U}$. 于是 $\mathbf{Q}_p^*\simeq\mathbf{Z}\times\mathbf{U}$. 进而由命题 7 证明了

$$\mathbf{U}=\mathbf{V}\times\mathbf{U}_1,$$

其中 $\mathbf{V}$ 为 $p-1$ 阶循环群, 而 $\mathbf{U}_1$ 的结构由命题 8 给出.

3.3. $\mathbf{Q}_p^*$ 中平方元素

定理 3 设 $p\neq 2$, 而 $x=p^n u\in\mathbf{Q}_p^*$, 其中 $n\in\mathbf{Z}$, $u\in\mathbf{U}$. 则 x 为平方元素的充要条件是 n 为偶数并且 u 在 $\mathbf{F}_p^*=\mathbf{U}/\mathbf{U}_1$ 中的象 $\bar{u}$ 是平方元素.

(后一条件意味着 $\bar{u}$ 的 Legendre 符号 $\left(\frac{\bar{u}}{p}\right)=1$. 以下我们用 $\left(\frac{u}{p}\right)$ 代替 $\left(\frac{\bar{u}}{p}\right)$.)

证 将 u 分解成形式 $u=v\cdot u_1$, 其中 $v\in\mathbf{V}$, $u_1\in\mathbf{U}_1$. 定

理 2 中的分解式 $\mathbf{Q}_p^* \simeq \mathbf{Z}\times\mathbf{V}\times\mathbf{U}_1$ 表明 x 是平方元素 $\Leftrightarrow n$ 为偶数并且 v 和 u_1 是平方元素. 但是 $\mathbf{U}_1$ 同构于 $\mathbf{Z}_p$ 而 2 为 $\mathbf{Z}_p$ 中可逆元素，故 $\mathbf{U}_1$ 中每个元素均是平方元素. 因为 $\mathbf{V}$ 同构于 $\mathbf{F}_p^*$，于是便得到定理.

系 如果 $p\neq 2$，则群 $\mathbf{Q}_p^*/\mathbf{Q}_p^{*2}$ 是型为 (2, 2) 的群. 它有代表元集 $\{1, p, u, up\}$，其中 $u\in\mathbf{U}$ 满足

$$\left(\frac{u}{p}\right)=-1.$$

证 这是显然的.

定理 4 $\mathbf{Q}_2^*$ 中元素 $x=p^n u$ 是平方元素的充要条件是 n 为偶数并且 $u\equiv 1 \pmod 8$.

证 分解式 $\mathbf{U}=\{\pm 1\}\times\mathbf{U}_2$ 表明 u 为平方元素 $\Leftrightarrow u\in\mathbf{U}_2$ 并且是 $\mathbf{U}_2$ 中平方元素. 现在，命题 8 的证明过程中所构作的同构 $\theta: \mathbf{Z}_2\to\mathbf{U}_2$ 将 $2^n\mathbf{Z}_2$ 映到 $\mathbf{U}_{n+2}$ 之上. 取 $n=1$，我们看到 $\mathbf{U}_2$ 中的平方元素集合是 $\mathbf{U}_3$. 于是元素 $u\in\mathbf{U}$ 为平方元素的充要条件是 $u\equiv 1 \pmod 8$，于是证明了定理.

注 将定理 1 的系 3 用于二次型 X^2，也可以证明 $\mathbf{U}_3$ 中每个元素都是平方元素.

系 群 $\mathbf{Q}_2^*/\mathbf{Q}_2^{*2}$ 的型为 (2, 2, 2). 它有代表元集 $\{\pm 1, \pm 5, \pm 2, \pm 10\}$.

证 这是因为 $\{\pm 1, \pm 5\}$ 是 $\mathbf{U}/\mathbf{U}_3$ 的代表元集.

注 1) 对于 $p=2$，用第一章 §3.2 中的公式定义同态 $\varepsilon, \omega: \mathbf{U}/\mathbf{U}_3\to\mathbf{Z}/2\mathbf{Z}$，即

$$\varepsilon(z)\equiv\frac{z-1}{2} \pmod 2=\begin{cases}0, & \text{如果 } z\equiv 1 \pmod 4,\\ 1, & \text{如果 } z\equiv -1 \pmod 4.\end{cases}$$

$$\omega(z)\equiv\frac{z^2-1}{8} \pmod 2=\begin{cases}0, & \text{如果 } z\equiv \pm 1 \pmod 8,\\ 1, & \text{如果 } z\equiv \pm 5 \pmod 8.\end{cases}$$

映射 ε 定义了 $\mathbf{U}/\mathbf{U}_2$ 到 $\mathbf{Z}/2\mathbf{Z}$ 之上的同构，而映射 ω 定义了 $\mathbf{U}_2/\mathbf{U}_3$ 到 $\mathbf{Z}/2\mathbf{Z}$ 之上的同构．因此 (ε, ω) 定义了 $\mathbf{U}/\mathbf{U}_3$ 到 $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$ 之上的同构．特别地，一个 2-adic 单位 z 是平方元素的充要条件是 $\varepsilon(z)=\omega(z)=0$．

2) 定理 3 和定理 4 表明 $\mathbf{Q}_p^{*2}$ 是 $\mathbf{Q}_p^*$ 的开子群．

第三章 Hilbert 符号

§1. 局部性质

在本节中，k 表示实数域 $\mathbf{R}$ 或者 p-adic 数域 $\mathbf{Q}_p$(其中 p 是素数).

1.1. 定义和简单性质

设 $a, b\in k^*$. 令

$$(a, b)=\begin{cases}1, & \text{如果 } z^2-ax^2-by^2=0 \text{ 在 } k^3 \text{ 中有解} \\ & \quad (z, x, y)\neq(0, 0, 0), \\ -1, & \text{否则,}\end{cases}$$

数 $(a, b)=\pm1$ 叫作 a 和 b 对于 k 的 Hilbert 符号. 显然，当 a 和 b 乘以平方元素时，(a, b) 不变. 因此 Hilbert 符号是从 $k^*/k^{*2}\times k^*/k^{*2}$ 到 $\{\pm1\}$ 的映射.

命题 1 设 $a, b\in k^*$ 而令 $k_b=k(\sqrt{b})$. 则 $(a, b)=1$ 的充要条件是 a 属于 k_b^* 的元素的范群 Nk_b^*.

证 如果 b 是元素 $c\in k$ 的平方，则方程 $z^2-ax^2-by^2=0$ 有解 $(c, 0, 1)$，于是 $(a, b)=1$. 对于这种情形，命题显然成立，因为 $k_b=k$ 而 $Nk_b^*=k^*$. 否则的话，k_b 是 k 的二次扩域. 以 β 表示 b 的一个平方根，每个元素 $\xi\in k_b$ 均可写成 $z+\beta y$，其中 $y, z\in k$，而 ξ 的范 $N(\xi)=z^2-by^2$. 如果 $a\in Nk_b^*$，则存在 $y, z\in k$，使 $a=z^2-by^2$，从而二次型 $z^2-ax^2-by^2$ 有零点 $(z, 1, y)$，于是我们有 $(a, b)=1$.

反之，如果 $(a, b)=1$，上面的二次型有零点

$$(z, x, y) \neq (0, 0, 0).$$

我们有 $x\neq 0$, 因为否则 b 将为平方元素. 由此看到 a 是元素 $\frac{z}{x}+\beta\frac{y}{x}$ 的范.

命题 2 Hilbert 符号满足下列公式:

i) $(a, b)=(b, a)$, $(a, c^2)=1$,

ii) $(a, -a)=1$, $(a, 1-a)=1$,

iii) $(a, b)=1 \Rightarrow (aa', b)=(a', b)$,

iv) $(a, b)=(a, -ab)=(a, (1-a)b)$.

(在这些公式中, a, a', b, c 表示 k^* 中元素. 如果公式中包含 $1-a$ 这一项时, 我们假定 $a\neq 1$.)

证 i) 是显然的. 如果 $b=-a$ (或者如果 $b=1-a$), 则二次型 $z^2-ax^2-by^2$ 有零点 $(0, 1, 1)$ (或者 $(1, 1, 1)$). 因此 $(a, b)=1$, 这就证明了 ii). 如果 $(a, b)=1$, 由命题 1 可知 a 在子群 Nk_b^* 之中. 于是 $a'\in Nk_b^* \Leftrightarrow aa'\in Nk_b^*$, 这就证明了 iii). 公式 iv) 由 i), ii) 和 iii) 推出.

注 公式 iii) 是公式

v) $(aa', b)=(a, b)(a', b)$

的特殊情形. 后者表达出 Hilbert 符号是双线性的, 这个公式将在下一节中证明.

1.2. (a, b) 的计算

定理 1 假若 $k=\mathbf{R}$, 我们有

$$(a, b)=\begin{cases} 1, & \text{如果 } a \text{ 或者 } b>0, \\ -1, & \text{如果 } a \text{ 和 } b \text{ 均} <0. \end{cases}$$

假若 $k=\mathbf{Q}_p$, 令 $a=p^{\alpha}u$, $b=p^{\beta}v$, 其中 u 和 v 属于 p-adic 单位群 $\mathbf{U}$, 我们有

$$(a, b)=\begin{cases}(-1)^{\alpha\beta\varepsilon(p)}\left(\dfrac{u}{p}\right)^{\beta}\left(\dfrac{v}{p}\right)^{\alpha}, & \text{如果 } p\neq 2,\\ (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)}, & \text{如果 } p=2.\end{cases}$$

$\Big[$注意$\left(\dfrac{u}{p}\right)$表示 Legendre 符号$\left(\dfrac{\bar{u}}{p}\right)$，其中 $\bar{u}$ 为 u 在 $\bmod p$ 约化同态：$\mathbf{U}\to\mathbf{F}_p^*$ 下之象．而 $\varepsilon(u)$ 和 $\omega(u)$ 分别代表 $\dfrac{u-1}{2}$ 和 $\dfrac{u^2-1}{8}$ 的 mod 2 同余类，见第二章 §3.3.$\Big]$

定理 2 Hilbert 符号是 $\mathbf{F}_2$-向量空间 k^*/k^{*2} 上的非退化双线性型．

[(a, b)的双线性恰好是 §1.1 末尾所提到的公式 v)．而"(a, b)是非退化的"意味着：如果 $b\in k^*$，使得对于每个 $a\in k^*$ 均有 $(a, b)=1$，则 $b\in k^{*2}$.]

系 如果 b 不为平方元素，则命题 1 中的群 Nk_b^* 是 k^* 的指数为 2 的子群．

证 根据命题 1，由 $\phi_b(a)=(a, b)$定义的同态 ϕ_b: $k^*\to\{\pm1\}$的核为 Nk_b^*．由于(a, b)是非退化的，从而 ϕ_b 是映上的．于是 ϕ_b 定义了 k^*/Nk_b^* 到 $\{\pm1\}$ 之上的同构．由此即得到本系．

注 更一般地，设 L 是 k 的有限 Galois 扩张，其 Galois 群是交换群．可以证明 k^*/NL^* 同构于 G，并且群 NL^* 的知识可以决定 L．这是"局部类域论"的两个主要结果．

定理 1 和定理 2 的证明．

情形 $k=\mathbf{R}$ 是显然的，然后注意 k^*/k^{*2} 是域 $\mathbf{F}_2$ 上一维向量空间，而 $\{1, -1\}$ 是代表元集．

现在设 $k=\mathbf{Q}_p$.

引理 设 $v\in\mathbf{U}$ 是 p-adic 单位．如果方程

$$z^2-px^2-vy^2=0$$

在 $\mathbf{Q}_p$ 中有非平凡解，则它有一解 (z, x, y)，使 $z, y \in \mathbf{U}$ 而 $x \in \mathbf{Z}_p$.

证 按照第二章 §2.1 的命题 6. 所给方程有本原解 (z, x, y). 让我们证明这个解即有所需性质. 如果不然，则或者 $y \equiv 0 \pmod p$，或者 $z \equiv 0 \pmod p$. 因为 $z^2 - vy^2 \equiv 0 \pmod p$ 而 $v \not\equiv 0 \pmod p$，我们便同时有 $y \equiv 0 \pmod p$ 和 $z \equiv 0 \pmod p$，于是 $px^2 \equiv 0 \pmod{p^2}$，即 $x \equiv 0 \pmod p$，这与 (z, x, y) 的本原性相矛盾.

现在回到定理 1 的证明上来，先设 $p \neq 2$.

显然可以只考虑指数 α 和 β 的 mod 2 剩余. 又由于 Hilbert 符号的对称性，从而只需考虑以下三种情形：

1) $\alpha = 0, \beta = 0$. 我们要证明 $(u, v) = 1$. 现在方程

$$z^2 - ux^2 - vy^2 = 0$$

有非平凡的 mod p 解（第一章 §2 定理 3 系 2）. 由于这个二次型的判别式是 p-adic 单位，上述解可以提升成 p-adic 解（第二章 §2.2 定理 1 系 2），从而 $(u, v) = 1$.

2) $\alpha = 1, \beta = 0$. 我们要证明 $(pu, v) = \left(\frac{v}{p}\right)$. 因为 $(u, v) = 1$，由命题 2 的公式 iii) 我们有 $(pu, v) = (p, v)$. 从而只需证明 $(p, v) = \left(\frac{v}{p}\right)$. 如果 v 为平方元素，这是显然的，因为上式两边均为 1. 否则便有 $\left(\frac{v}{p}\right) = -1$.（见第二章 §3.3 定理 3.）这时上面引理表明 $z^2 - px^2 - vy^2$ 没有非平凡零点，于是 $(p, v) = -1$.

3) $\alpha = 1, \beta = 1$. 我们要证

$$(pu, pv) = (-1)^{\frac{p-1}{2}} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right).$$

命题 2 的公式 iv) 表明

$$(pu,\ pv)=(pu,\ -p^2uv)=(pu,\ -uv).$$

根据上面所述，我们有 $(pu,\ pv)=\left(\frac{-uv}{p}\right)$，由此再注意

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}},$$

即得所需结果.

这样我们就证明了定理 1 (对于 $p\neq 2$)，而定理 2 可以由它立刻推出来，因为公式表明 $(a,\ b)$ 是双线性的，为了证明其非退化性，只需证明对每个非平方元素 $a\in k^*$，均存在元素 b，使 $(a,\ b)=-1$. 按照第二章 §3.3 定理 3 的系，我们可取 $a=p$，u 或者 up，其中 $u\in\mathbf{U}$，$\left(\frac{u}{p}\right)=-1$. 这时我们取 b 分别为 u，p 或者 u 即可.

情形 $p=2$. 这时仍然只需考虑 α 和 β 的 mod 2 剩余，从而只需考虑三种情形：

1) $\alpha=0,\ \beta=0$. 我们必需证明

$$(u,\ v)=\begin{cases}1, & \text{如果 } u \text{ 或者 } v\equiv 1 \pmod 4,\\ -1, & \text{否则}.\end{cases}$$

先设 $u\equiv 1 \pmod 4$，则 $u\equiv 1 \pmod 8$ 或者 $u\equiv 5 \pmod 8$. 在第一种情形下 u 是平方元素(第二章 §3.3 定理 4)，于是我们有 $(u,\ v)=1$.. 在第二种情形下我们有 $u+4v\equiv 1 \pmod 8$，从而存在 $w\in\mathbf{U}$ 使 $w^2=u+4v$. 于是二次型 $z^2-ux^2-vy^2$ 有零点 $(w, 1, 2)$，即有 $(u,\ v)=1$. 现在让我们假定

$$u\equiv v\equiv -1 \pmod 4.$$

如果 $(z,\ x,\ y)$ 是 $z^2-ux^2-vy^2=0$ 的本原解，则

$$z^2+x^2+y^2\equiv 0 \pmod 4.$$

但是 $\mathbf{Z}/4\mathbf{Z}$ 的平方元素是 0 和 1，因此上面同余式导出 x, y,

z 均同余于 $0 \pmod 2$，这与本原性假设相矛盾．因此对于这种情形我们有 $(u,\ v)=-1$.

2) $\alpha=1,\ \beta=0$．我们必需证明

$$(2u,\ v)=(-1)^{\varepsilon(u)\varepsilon(v)+\omega(v)}.$$

首先让我们证明 $(2,\ v)=(-1)^{\omega(v)}$，即证明 $(2,\ v)=1$ 等价于 $v\equiv\pm1 \pmod 8$．根据上述引理，如果 $(2,\ v)=1$，则存在 $x,\ y,\ z\in \mathbf{Z}_2$，使 $z^2-2x^2-vy^2=0$ 并且 $y,\ z\not\equiv 0 \pmod 2$．于是我们有 $y^2\equiv z^2\equiv 1 \pmod 8$，从而 $1-2x^2-v\equiv 0 \pmod 8$．但是 mod 8 平方元素只有 0, 1 和 4，由此推出 $v\equiv\pm1 \pmod 8$．反之，如果 $v\equiv 1 \pmod 8$，v 是平方元素，从而 $(2,\ v)=1$．如果 $v\equiv -1 \pmod 8$，则方程 $z^2-2x^2-vy^2=0$ 有 mod 8 解 $(1, 1, 1)$．这个近似解可以提升成真正解(第二章 §2.2，定理 1 的系 3)，于是 $(2,\ v)=1$.

其次我们证明 $(2u,\ v)=(2,\ v)(u,\ v)$．根据命题 2，如果 $(2,\ v)=1$ 或者 $(u,\ v)=1$ 时，这公式是成立的．剩下的情形为 $(2,\ v)=(u,\ v)=-1$，即 $v\equiv 3 \pmod 8$，而 $u\equiv 3$ 或者 $-1 \pmod 8$．将 u 和 v 乘以平方元素之后，我们可以设 $u=-1$，$v=3$ 或者 $u=3,\ v=-5$．现在，方程

$$z^2+2x^2-3y^2=0 \quad 和 \quad z^2-6x^2+5y^2=0$$

均有解 $(1, 1, 1)$，于是我们有 $(2u,\ v)=1$.

3) $\alpha=1,\ \beta=1$．我们必需证明

$$(2u, 2v)=(-1)^{\varepsilon(u)\varepsilon(v)+\omega(u)+\omega(v)}.$$

命题 2 的公式 iv) 表明

$$(2u, 2v)=(2u,\ -4uv)=(2u,\ -uv).$$

由上所述，我们有

$$(2u, 2v)=(-1)^{\varepsilon(u)\varepsilon(-uv)+\omega(-uv)}.$$

因为 $\varepsilon(-1)=1,\ \omega(-1)=0,\ \varepsilon(u)(1+\varepsilon(u))=0$，从而上式

右边的指数是 $\varepsilon(u)\varepsilon(v)+\omega(u)+\omega(v)$，这就证明了定理 1. 由此公式以及 ε 和 ω 均是同态，即知 (a, b) 是双线性的. 对于非退化性，只需检查代表元集 $\{u, 2u \mid u=1, 5, -1, -5\}$ 即可. 事实上，我们有

$$(5, 2u)=-1, \quad 和 \quad (-1, -1)=(-1, -5)=-1.$$

注 将 (a, b) 写成形式 $(-1)^{[a,b]}$，其中 $[a, b]\in\mathbf{Z}/2\mathbf{Z}$. 则 $[a, b]$ 是 k^*/k^{*2} 上取值于 $\mathbf{Z}/2\mathbf{Z}$ 的对称双线性型，并且定理 1 给出它对于 k^*/k^{*2} 的某一组基的矩阵:

对于 $k=\mathbf{R}$，该矩阵为 (1).

对于 $k=\mathbf{Q}_p$，$p\neq 2$，取基 $\{p, u\}$，其中 $\left(\frac{u}{p}\right)=-1$，则当 $p\equiv 1 \pmod 4$ 时该矩阵为 $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$，当 $p\equiv 3 \pmod 4$ 时该矩阵为 $\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$.

对于 $k=\mathbf{Q}_2$，取基 $\{2, -1, 5\}$，该矩阵为 $\begin{pmatrix}0 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 0\end{pmatrix}$.

§2. 整体性质

有理数域 $\mathbf{Q}$ 作为子域可以嵌到每个域 $\mathbf{Q}_p$ 和 $\mathbf{R}$ 中. 如果 $a, b\in\mathbf{Q}^*$，我们以 $(a, b)_p$ 和 $(a, b)_\infty$ 分别表示它在 $\mathbf{Q}_p$ 和 $\mathbf{R}$ 中象元素的 Hilbert 符号. 我们定义 V 为全体素数加上符号 ∞ 所构成的集合，并约定命 $\mathbf{Q}_\infty=\mathbf{R}$，于是对于每个 $v\in V$，$\mathbf{Q}$ 在 $\mathbf{Q}_v$ 中是稠密的.

2.1. 乘积公式

定理 3(Hilbert) 如果 $a, b\in\mathbf{Q}^*$，则对几乎所有 $v\in V$

均有$(a, b)_v=1$，并且

$$\prod_{v\in V}(a, b)_v=1.$$

（"几乎所有 $v\in V$"的意思是："V 中除了有限多个之外的所有元素".）

证 由于 Hilbert 符号是双线性的，从而只需对 a 和 b 等于 -1 或素数时证明该定理即可. 在每种情形下，定理 1 均给出 $(a, b)_v$ 的值. 我们发现

1) $a=-1$, $b=-1$. 则 $(-1, -1)_\infty=(-1, -1)_2=-1$，而当 $p\neq\infty$, 2 时，$(-1, -1)_p=1$，从而乘积为 1.

2) $a=-1$, $b=l$, l 为素数. 如果 $l=2$，则对于每个 $v\in V$ 均有 $(-1, 2)_v=1$. 如果 $l\neq 2$，则当 $v\neq 2$ 和 l 时有 $(-1, l)_v=1$，而 $(-1, l)_2=(-1, l)_l=(-1)^{\varepsilon(l)}$，于是乘积等于 1.

3) $a=l$, $b=l'$，其中 l 和 l' 均是素数. 如果 $l=l'$，命题 2 的公式 iv) 表明对于每个 $v\in V$ 均有 $(l, l)_v=(-1, l)_v$，从而归结为上面所考虑过的情形. 如果 l 与 l' 不同而且均不为 2，则当 $v\neq 2$, l, l' 时，我们有 $(l, l')_v=1$，而

$$(l, l')_2=(-1)^{\varepsilon(l)\varepsilon(l')},$$

$$(l, l')_l=\left(\frac{l'}{l}\right), \quad (l, l')_{l'}=\left(\frac{l}{l'}\right),$$

但是由二次互反律（第一章 § 3.3 定理 6）我们有

$$\left(\frac{l'}{l}\right)\left(\frac{l}{l'}\right)=(-1)^{\varepsilon(l)\varepsilon(l')},$$

从而乘积等于 1. 如果 $l\neq l'$ 并且 $l'=2$，则当 $v\neq 2$, l 时我们有 $(l, 2)_v=1$，而

$$(l, 2)_2=(-1)^{\omega(l)}, \quad (l, 2)_l=\left(\frac{2}{l}\right)=(-1)^{\omega(l)}.$$

见第一章 § 3.2 定理 5，从而乘积为 1，这就完成了证明.

注 乘积公式本质上等价于二次互反律. 它的益处主要是基于如下的事实，即它可以推广到一切代数数域中(集合 V 改成域的全部"位"所组成的集合).

2.2. 具有给定 Hilbert 符号的有理数之存在性

定理 4 设 $(a_i)_{i\in I}$ 是 $\mathbf{Q}^*$ 中元素的有限集，而 $(\varepsilon_{i,v})_{i\in I, v\in V}$ 是一个数集合，每个 $\varepsilon_{i,v}$ 均是 $+1$ 或 -1. 为了存在元素 $x\in\mathbf{Q}^*$，使 $(a_i, x)_v=\varepsilon_{i,v}$ (对一切 $i\in I$, $v\in V$)，其充要条件是下述诸条件满足:

(1) 几乎所有的 $\varepsilon_{i,v}$ 均等于 1.

(2) 对每个 $i\in I$ 均有 $\prod_{v\in V}\varepsilon_{i,v}=1$.

(3) 对每个 $v\in V$，均存在 $x_v\in\mathbf{Q}_v^*$ 使 $(a_i, x_v)_v=\varepsilon_{i,v}$ (对一切 $i\in I$).

证 (1)和(2)的必要性从定理 3 推出；而(3)的必要性是显然的(取 $x_v=x$).

为证这些条件的充分性，我们需要如下三条引理:

引理 1(中国剩余定理) 设 $a_1, \cdots, a_n, m_1, \cdots, m_n$ 是整数，并且 m_i 两两互素. 则存在整数 a，使对每个 i 均有 $a\equiv a_i \pmod{m_i}$.

证 设 m 是诸 m_i 之积. Bezout 定理表明正则同态

$$\mathbf{Z}/m\mathbf{Z}\to\prod_{i=1}^{n}\mathbf{Z}/m_i\mathbf{Z}$$

是同构. 由此即得引理.

引理 2("逼近定理") 设 S 是 V 的有限子集合. 则 $\mathbf{Q}$ 在 $\prod_{v\in S}\mathbf{Q}_v$ 中的象在这一积集 $\prod_{v\in S}\mathbf{Q}_v$ 中稠密(对于 $\mathbf{Q}_v$ 中拓扑之积拓扑).

证　因为可以任意扩大 S, 我们可以设

$$S=\{\infty, p_1, \cdots, p_n\},$$

其中 p_i 是不同的素数, 我们必需证明 $\mathbf{Q}$ 在 $\mathbf{R}\times\mathbf{Q}_{p_1}\times\cdots\times\mathbf{Q}_{p_n}$ 中稠密. 设 $(x_\infty, x_1, \cdots, x_n)$ 是该积集中一点, 我们来证明这个点是 $\mathbf{Q}$ 的附着点. 乘以某个整数之后, 我们可设 $x_i\in\mathbf{Z}_{p_i}$ $(1\leqslant i\leqslant n)$. 现在必需证明对每个 $\varepsilon>0$ 和每个整数 $N>0$, 均存在 $x\in\mathbf{Q}$, 使

$$|x-x_\infty|\leqslant\varepsilon \quad 并且 \quad v_{p_i}(x-x_i)\geqslant N \quad (1\leqslant i\leqslant n).$$

将引理 1 用于 $m_i=p_i^N$, 可知存在 $x_0\in\mathbf{Z}$, 使 $v_{p_i}(x_0-x_i)\geqslant N$ (对一切 i). 现在取一整数 $q\geqslant 2$, 使 q 与所有 p_i 均互素 (例如取一个充分大的素数). 形如 a/q^m $(a\in\mathbf{Z}, m\geqslant 0)$ 的有理数在 $\mathbf{R}$ 中稠密 (这是因为当 $m\to\infty$ 时 $q^m\to\infty$). 取一数 $u=a/q^m$ 使

$$|x_0-x_\infty+up_1^N\cdots p_n^N|\leqslant\varepsilon,$$

则有理数 $x=x_0+up_1^N\cdots p_n^N$ 即有所需性质.

引理 3 (Dirichlet 定理)　如果 a 和 m 是彼此互素并均 $\geqslant 1$ 的整数, 则存在无穷多个素数 p 使 $p\equiv a \pmod m$.

证明将在第六章中给出. 读者可以看出它并没有用到第三、四和五章的结果.

现在回到定理 4, 令 $(\varepsilon_{i,v})$ 是等于 ± 1 的数的集合并且满足条件(1), (2)和(3). 将 a_i 乘以某个整数的平方之后, 我们可以假定所有的 a_i 均是整数. 令 S 为 V 的子集, 由 ∞, 2 和 a_i 的素因子所构成. 令 $T=\{v\in V\,|\,存在\ i\in I\ 使\ \varepsilon_{i,v}=-1\}$. 这两个集合均是有限的. 我们分两种情形考虑:

1) $S\cap T=\emptyset$.

令

$$a=\prod_{\substack{l\in T\\ l\neq\infty}} l, \quad m=8\prod_{\substack{l\in S\\ l\neq 2,\infty}} l.$$

因为 $S\cap T=\emptyset$, 整数 a 和 m 互素, 并且由引理 3 可知存在素数 $p\equiv a \pmod m$, 其中 $p\notin S\cup T$. 现在证明 $x=ap$ 有所需性质, 即 $(a_i, x)_v=\varepsilon_{i,v}$ 对一切 $i\in I$ 和 $v\in V$.

如果 $v\in S$, 由于 $S\cap T=\emptyset$, 我们有 $\varepsilon_{i,v}=1$, 从而必需证明 $(a_i, x)_v=1$. 如果 $v=\infty$, 由 $x>0$ 即得结论. 如果 v 为素数 l, 我们有 $x\equiv a^2 \pmod m$, 从而对于 $l=2$ 有 $x\equiv a^2 \pmod 8$, 而对于 $l\neq 2$ 有 $x\equiv a^2 \pmod l$. 因为 x 和 a 均是 l-adic 单位, 这表明 x 是 $\mathbf{Q}^*$ 中的平方元素(见第二章 § 3.3), 于是有

$$(a_i, x)_v=1.$$

如果 $v=l\notin S$, a_i 是 l-adic 单位. 由于 $l\neq 2$, 我们有

$$(a_i, b)_l=\left(\frac{a_i}{l}\right)^{v_l(b)} \quad (\text{对一切 } b\in\mathbf{Q}_l^*),$$

见定理 1. 如果 $l\notin T\cup\{p\}$, x 是 l-adic 单位, 于是 $v_l(x)=0$, 而上面公式表明 $(a_i, x)_l=1$. 另一方面我们有 $\varepsilon_{i,l}=1$, 这是因为 $l\notin T$. 如果 $l\in T$, 我们有 $v_l(x)=1$, 并且条件(3)表明存在 $x_l\in\mathbf{Q}_l^*$ 使 $(a_i, x_l)_l=\varepsilon_{i,l}$ (对于一切 $i\in I$). 由于有某个 $\varepsilon_{i,l}=-1$(因为 $l\in T$), 我们有 $v_l(x_l)\equiv 1 \pmod 2$, 从而

$$(a_i, x)_l=\left(\frac{a_i}{l}\right)=(a_i, x_l)_l=\varepsilon_{i,l} \quad (\text{对一切 } i\in I).$$

只剩下情形 $l=p$, 这可由其余等式利用如下乘积公式推出:

$$(a_i, x)_p=\prod_{v\neq p}(a_i, x)_v=\prod_{v\neq p}\varepsilon_{i,v}=\varepsilon_{i,p}.$$

这就对于 $S\cap T=\emptyset$ 的情形完成了定理 4 的证明.

2) 一般情形.

我们知道, $\mathbf{Q}_v^*$ 的平方元素形成 $\mathbf{Q}_v^*$ 的开子群, 见第二章 § 3.3. 由引理 2, 存在 $x'\in\mathbf{Q}^*$ 使对于每个 $v\in S$, x'/x_v 是 $\mathbf{Q}_v^*$ 中平方元素. 特别地, 对于每个 $v\in S$ 均有

$$(a_i,\ x')_v=(a_i,\ x_v)_v=\varepsilon_{i,v}.$$

如果令 $\eta_{i,v}=\varepsilon_{i,v}(a_i,\ x')_v$，那末集合$(\eta_{i,v})$也满足条件(1)、(2)和(3)，并且若 $v\in S$，则 $\eta_{i,v}=1$. 由上面的1)可知存在 $y\in\mathbf{Q}^*$ 使得对每个 $i\in I$ 和 $v\in V$ 均有$(a_i,\ y)_v=\eta_{i,v}$. 如果令 $x=yx'$，显然 x 即有所需要的性质.

第四章　$\mathbf{Q}_p$ 和 $\mathbf{Q}$ 上的二次型

§1. 二　次　型

1.1. 定义

首先提一下二次型的一般概念(见 Bourbaki: 代数, 第九章, 3, n°4).

定义 1　设 V 是交换环 A 上的模. 函数 $Q: V \to A$ 叫作 V 上的二次型, 如果

1) $Q(ax) = a^2 Q(x)$, $a \in A$, $x \in V$.

2) 函数 $(x, y) \mapsto Q(x+y) - Q(x) - Q(y)$ 是双线性型.

这样的 (V, Q) 称作一个二次模. 在本章中, 我们限定在环 A 为特征 $\neq 2$ 的域 k 这一情形. 这时, A-模 V 是 k-向量空间. 我们假设它的维数是有限的.

我们令:

$$x \cdot y = \frac{1}{2}\{Q(x+y) - Q(x) - Q(y)\}.$$

由于 k 的特征 $\neq 2$, 从而这是有意义的. 映射 $(x, y) \mapsto x \cdot y$ 是 V 上的对称双线性型, 叫作与 Q 相结合的内积. 这就构造出在二次型和对称双线性型之间的一个一一对应(在特征 2 的时候情况并不如此).

如果 (V, Q) 和 (V', Q') 是两个二次模, 线性映射 $f: V \to V'$ 称作是从 (V, Q) 到 (V', Q') 中的同态(或保距同态), 是指 $Q' \circ f = Q$. 这时有 $f(x) \cdot f(y) = x \cdot y$(对所有的 x, $y \in V$).

二次型的矩阵. 设 $(e_i)_{1 \leqslant i \leqslant n}$ 是 V 的一组基. Q 对于这组

基的矩阵是 $A=(a_{ij})$，其中 $a_{ij}=e_i\cdot e_j$. 它是对称矩阵. 如果 $x=\sum x_ie_i$ 是 V 中元素，则

$$Q(x)=\sum_{i,j}a_{ij}x_ix_j,$$

这表明 $Q(x)$ 是通常意义下关于 $x_1, \cdots, x_n$ 的二次型.

如果用一个可逆矩阵 X 改变基 (e_i)，那末 Q 对于新的一组基的矩阵是 $A'=XA{}^tX$，这里 ${}^tX$ 表示 X 的转置. 特别地，

$$\det(A')=\det(A)\det(X)^2,$$

这表明 $\det(A)$ 除了一个因子（它是 k^{*2} 中元素）外是完全确定的. 称它为 Q 的判别式，记成 $\operatorname{disc}(Q)$.

1.2. 正交性

设 (V, Q) 是 k 上的一个二次模. V 的两个元素 x, y 称作是正交的，如果 $x\cdot y=0$. 以 H^0 表示正交于 V 的子集 H 的全部元素所构成的集合，它是 V 的向量子空间. 假设 V_1 和 V_2 是 V 的向量子空间，称它们为正交的，如果 $V_1\subset V_2^0$，即如果 $x\in V_1$, $y\in V_2$，便导致 $x\cdot y=0$.

V 自身的正交补 V^0 叫作 V 的根子空间（或核子空间），记为 $\operatorname{rad}(V)$. 它的补维数（codimension）称作是 Q 的秩. 如果 $V^0=0$，我们称 Q 是非退化的，这等价于说 Q 的判别式 $\neq 0$（在这种情形下，我们将判别式看成是群 k^*/k^{*2} 中的元素）.

设 U 是 V 的向量子空间，令 U^* 为 U 的对偶. 又令 q_U: $V\to U^*$ 是如下的函数：它将每个 $x\in V$ 结合一个线性型 $(y\in U\mapsto x\cdot y)$. q_U 的核是 U^0. 特别地可以看出，Q 是非退化的 $\Leftrightarrow q_V$: $V\to V^*$ 是同构.

定义 2 设 $U_1, \cdots, U_m$ 是 V 的向量子空间. 称 V 是 U_i 的正交直和，如果它们两两正交并且 V 是它们的直和，这时可以写成

$$V=U_1\hat{\oplus}\cdots\hat{\oplus}U_m.$$

注 如果$x\in V$在U_i中分量为x_i，则

$$Q(x)=Q_1(x_1)+\cdots+Q_m(x_m),$$

其中$Q_i=Q|U_i$表示Q在U_i上的限制．反之，如果(U_i, Q_i)是一个二次模集合，上面的公式可使$V=\oplus U_i$具有二次型Q，称Q为Q_i的直和，并且有$V=U_1\hat{\oplus}\cdots\hat{\oplus}U_m$.

命题 1 如果U是$\mathrm{rad}(V)$在V中的补子空间，则

$$V=U\hat{\oplus}\mathrm{rad}(V).$$

这是显然的．

命题 2 假设(V, Q)是非退化的，则

i) V到一个二次模(V', Q')中的每个保距同态均是单射．

ii) 对于V的每个子空间U，都有

$$U^{00}=U,\quad \dim U+\dim U^0=\dim V,$$

$$\mathrm{rad}(U)=\mathrm{rad}(U^0)=U\cap U^0.$$

二次模U是非退化的$\Leftrightarrow U^0$非退化．并且这时$V=U\hat{\oplus}U^0$.

iii) 如果V是两个子空间的正交和，则这两个子空间均非退化，并且彼此正交．

证 如果$f: V\to V'$是保距同态并且$f(x)=0$，我们有

$$x\cdot y=f(x)\cdot f(y)=0\quad（对一切\ y\in V）.$$

这导致$x=0$，因为(V, Q)是非退化的．

如果U是V的向量子空间，上面定义的同态$q_U: V\to U^*$是映上的．事实上，它是$q_V: V\to V^*$与正则映上$V^*\to U^*$的合成，而我们已经假定q_V是一一映射．因此有正合列：

$$0\to U^0\to V\to U^*\to 0,$$

于是 $\qquad \dim V=\dim U^*+\dim U^0=\dim U+\dim U^0.$

这就证明了U和U^{00}有同样的维数．因为$U\subseteq U^{00}$，我们有$U=U^{00}$．公式$\mathrm{rad}(U)=U\cap U^0$是显然的．将此式用于$U^0$

并考虑到$U^{00}=U$，我们得到$\mathrm{rad}(U^0)=\mathrm{rad}(U)$，并且同时给出 ii) 的最后论断．最后，iii) 是显然的．

1.3．迷向向量

定义 3 二次模 (V, Q) 的元素 x 叫作是迷向的，如果 $Q(x)=0$．V 的子空间 U 叫作是迷向的，如果它的每个元素都是迷向的．

显然有

$$U \text{ 迷向} \Leftrightarrow U\subset U^0 \Leftrightarrow Q|U=0.$$

定义 4 一个二次模如果有由两个迷向元素 x 和 y 形成的一组基，并且 $x\cdot y\neq 0$，便称此二次模为双曲平面．

将 y 乘以 $1/x\cdot y$ 之后，我们可设 $x\cdot y=1$．这时该二次型对于 x, y 的矩阵为 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 这样简单的形式．它的判别式是 -1（特别地，它非退化）．

命题 3 设 x 是非退化二次模 (V, Q) 中的非零迷向元素，则 V 存在子空间 U，使 $x\in U$ 并且 U 是双曲平面．

证 由于 V 非退化，从而存在 $z\in V$ 使得 $x\cdot z=1$．元素 $y=2z-(z\cdot z)x$ 为迷向的，并且 $x\cdot y=2$．空间 $U=kx+ky$ 即有所需性质．

系 如果 (V, Q) 非退化并且包含非零迷向元素，则

$$Q(V)=k.$$

（换句话说，对每个 $a\in k$，均存在 $v\in V$ 使得 $Q(v)=a$．）

证 根据命题 3，可设 V 为双曲平面．设 V 有基 x, y．其中 $x\cdot y=1$ 并且 x 和 y 均迷向．如果 $a\in k$，那末

$$a=Q\left(x+\frac{a}{2}y\right),$$

由此可知 $Q(V)=k$.

1.4. 正交基

定义 5 二次模 (V, Q) 的基 $(e_1, \cdots, e_n)$ 称作是正交的，如果元素 e_i 两两正交，即如果 $V=ke_1\hat{\oplus}\cdots\hat{\oplus}ke_n$.

这可以说成，Q 对于这组基的矩阵是对角阵

$$\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ 0 & 0 & \cdots & a_n \end{pmatrix}.$$

如果 $x=\sum x_ie_i$，我们有 $Q(x)=a_1x_1^2+\cdots+a_nx_n^2$.

定理 1 每个二次模 (V, Q) 均有正交基.

证 我们对 $n=\dim V$ 归纳，$n=0$ 的情形是显然的. 如果 V 迷向，V 的每组基均正交. 否则，取一元素 $e_1\in V$，使 $e_1\cdot e_1\neq 0$. e_1 的正交补 H 是超平面. 由于 $e_1\notin H$，我们有

$$V=ke_1\oplus H.$$

按照归纳假设，H 有正交基 $(e_2, \cdots, e_n)$，于是 $(e_1, e_2, \cdots, e_n)$ 即有所需性质.

定义 6 V 的两组正交基

$$\boldsymbol{e}=(e_1, \cdots, e_n), \quad \boldsymbol{e}'=(e'_1, \cdots, e'_n)$$

叫作是毗连的，如果它们有公共元素(即如果存在 i 和 j，使得 $e_i=e'_j$).

定理 2 设 (V, Q) 是维数 $\geqslant 3$ 的二次模，令

$$\boldsymbol{e}=(e_1, \cdots, e_n), \quad \boldsymbol{e}'=(e'_1, \cdots, e'_n)$$

是 V 的两组正交基，则 V 存在正交基的有限序列 $\boldsymbol{e}^{(0)}$, $\boldsymbol{e}^{(1)}$, $\cdots$, $\boldsymbol{e}^{(m)}$，使 $\boldsymbol{e}^{(0)}=\boldsymbol{e}$, $\boldsymbol{e}^{(m)}=\boldsymbol{e}'$，并且对于 $0\leqslant i<m$, $\boldsymbol{e}^{(i)}$ 与 $\boldsymbol{e}^{(i+1)}$ 相毗连.

（我们称 $\mathbf{e}^{(0)}, \cdots, \mathbf{e}^{(m)}$ 为从 $\mathbf{e}$ 到 $\mathbf{e}'$ 的正交基毗连链.）

证(*) 我们分三种情形考虑:

i) $(e_1\cdot e_1)(e_1'\cdot e_1')-(e_1\cdot e_1')^2\neq 0$.

这就是说，e_1 和 e_1' 不成比例并且平面 $P=ke_1+ke_1'$ 是非退化的. 于是存在 ε_2 和 ε_2' 使得

$$P=ke_1\hat{\oplus}k\varepsilon_2 \quad 并且 \quad P=ke_1'\hat{\oplus}k\varepsilon_2'.$$

设 H 是 P 的正交补. 由于 P 非退化，我们有 $V=H\oplus P$（见命题 2）. 令 $(e_3'', \cdots, e_n'')$ 是 H 的正交基，我们便有从 $\mathbf{e}$ 到 $\mathbf{e}'$ 的正交基毗连链:

$$\mathbf{e}\rightarrow(e_1, \varepsilon_2, e_3'', \cdots, e_n'')\rightarrow(e_1', \varepsilon_2', e_3'', \cdots, e_n'')\rightarrow\mathbf{e}'.$$

从而对于这种情形证明了定理.

ii) $(e_1\cdot e_1)(e_2'\cdot e_2')-(e_1\cdot e_2')^2\neq 0$.

将 e_1' 改成 e_2' 然后类似地证明.

iii) $(e_1\cdot e_1)(e_i'\cdot e_i')-(e_1\cdot e_i')^2=0 \quad (i=1, 2)$.

我们首先证明:

引理 存在 $x\in k$，使 $e_x=e_1'+xe_2'$ 非迷向，并且与 e_1 生成非退化平面.

证 我们有 $e_x\cdot e_x=e_1'\cdot e_1'+x^2(e_2'\cdot e_2')$. 因此我们必需取

$$x^2\neq-(e_1'\cdot e_1')/(e_2'\cdot e_2').$$

此外，为了 e_x 与 e_1 生成非退化平面，其充要条件是

$$(e_1\cdot e_1)(e_x\cdot e_x)-(e_1\cdot e_x)^2\neq 0.$$

如果我们把上式左边算出来，考虑到假设条件 iii)，便会

(*) 证明中用到了条件: $e_1\cdot e_1\neq 0$, $e_1'\cdot e_1'\neq 0$, $e_2'\cdot e_2'\neq 0$. 当 V 的秩 $\geqslant 2$ 时，改变一下标号，总可以选取 e_1, e_1', e_2' 满足此条件. 当 V 的秩 $\leqslant 1$ 时，易知定理 2 成立. ——译者注

发现它是 $-2x(e_1\cdot e'_1)(e_1\cdot e'_2)$. 现在假设条件 iii) 导致

$$e_1\cdot e_i\neq 0 \quad (i=1,\ 2).$$

因此我们看出 e_x 满足引理条件 $\Leftrightarrow x\neq 0$ 并且

$$x^2\neq -(e_1\cdot e_1)/(e_2\cdot e_2).$$

这至多排除掉 x 的三个值. 如果 k 至少有 4 个元素, 我们可以找到这样的 x. 于是只剩下 $k=\mathbf{F}_3$ 的情形(由于 $\mathrm{char}(k)\neq 2$, 从而 $k=\mathbf{F}_2$ 的情形被排除掉). 但是这时, 每个非零元素的平方均为 1, 从而假设条件 iii) 可以写成

$$(e_1\cdot e_1)(e'_i\cdot e'_i)=1 \quad (i=1,\ 2).$$

因此
$$(e'_1\cdot e'_1)/(e'_2\cdot e'_2)=1,$$
为了满足条件 $x^2\neq 0, -1$, 只需取 $x=1$ 即可.

这表明取 $e_x=e'_1+xe'_2$, 则引理条件成立. 由于 e_x 非迷向, 从而存在 e''_2, 使 $(e_x,\ e''_2)$ 为 $ke'_1\oplus ke'_2$ 的正交基. 令

$$\boldsymbol{e}''=(e_x,\ e''_2,\ e'_3,\ \cdots,\ e'_n).$$

这是 V 的一组正交基. 由于 ke_1+ke_x 是非退化平面, 本证明的 i) 部分表明可以得到从 $\boldsymbol{e}$ 到 $\boldsymbol{e}''$ 的正交基毗连链. 又由于 $\boldsymbol{e}'$ 和 $\boldsymbol{e}''$ 是毗连的, 从而即得定理.

1.5. Witt 定理

令 $(V,\ Q)$ 和 $(V',\ Q')$ 是两个非退化的二次模. 令 U 为 V 的子空间, 而

$$s:\ U\rightarrow V'$$

是从 U 到 V' 中的单射保距同态. 我们希望把 s 扩充到比 U 大的子空间上, 如果可能, 希望扩充到整个 V 上. 我们从 U 退化这一情形开始:

引理 如果U退化，我们可以将s扩充成单射保距同态$s_1: U_1 \to V'$，其中U为U_1的超平面.

证(*) 设x为$\mathrm{rad}(U)$中的非零元素. 由于x迷向，根据命题3，存在V的双曲平面包含x. 于是可找到$y\in V$，使$x\cdot y=1$，$y\cdot y=0$. 由于y不与x正交，我们有$y\notin U$，而U是子空间$U_1=U\oplus ky$的超平面. 类似地，我们构造元素$y'\in V'$，使$s(x)\cdot y'=1$，$y'\cdot y'=0$. 令$s_1: U_1\to V'$是线性映射，它在U上与s一致，而将y映成y'. 显然s_1即为所求.

定理3(Witt) 如果(V, Q)和(V', Q')是同构的非退化二次模，则V之子空间U的每个单射保距同态

$$s: \quad U\to V'$$

都可以扩充成V到V'上的一个保距同构.

证 因为V和V'同构，我们可设$V=V'$. 此外，利用上述引理，我们又归结到U非退化的情形. 现在我们对$\dim U$利用数学归纳法.

如果$\dim U=1$，U是由非迷向元素x生成的. 如果

$$y=s(x),$$

我们有$y\cdot y=x\cdot x$. 可以取$\varepsilon=\pm 1$，使$x+\varepsilon y$非迷向. 因否则我们将有

$$2x\cdot x+2x\cdot y=2x\cdot x-2x\cdot y=0,$$

这将导致$x\cdot x=0$. 取定这样的ε之后，令H为$z=x+\varepsilon y$的

(*) 原证明中对于y和y'的选取还不能保证扩充s_1的可定义性. 建议将证明修改如下:

取$x\in\mathrm{rad}(U)$，$x\neq 0$. 令$U=kx\hat{\oplus}W$，则$s(U)=ks(x)\hat{\oplus}s(W)$. 再取$y\in W^0\backslash U^0$，$y\neq 0$(这由命题2保证)，使$x\cdot y=1$. 类似地取

$$y'\in s(W)^0\backslash s(U)^0, \quad y'\neq 0,$$

使$y'\cdot s(x)=1$. 令U_1是U和y张成的向量空间，定义线性映射$s_1: U_1\to V'$，使$s_1|_U=s$，而$s_1(y)=y'$. 则s_1即为所求.——译者注

正交补. 我们有 $V=kz\oplus H$. 令 σ 为"关于 H 的反射", 即它是 V 的自同构, 在 H 上为恒等映射, 而将 z 映成 $-z$. 由于 $x-\varepsilon y\in H$, 我们有

$$\sigma(x-\varepsilon y)=x-\varepsilon y, \quad \sigma(x+\varepsilon y)=-x-\varepsilon y,$$

于是 $\sigma(x)=-\varepsilon y$, 从而自同构 $-\varepsilon\sigma$ 便是 s 的扩充.

如果 $\dim U>1$, 我们将 U 分解成形式 $U_1\hat{\oplus}U_2$, 其中 U_1, $U_2\neq 0$. 根据归纳假设, s 在 U_1 上的限制可以扩充成 V 的自同构 σ_1. 将 s 改成 $\sigma_1^{-1}\circ s$ 之后, 我们可以假定 s 在 U_1 上为恒等映射. 这时同态 s 将 U_2 映到 U_1 的正交补 V_1 之中. 根据归纳假设, s 在 U_2 上的限制可以扩充成 V_1 的自同构 σ_2. 设 σ 为 V 之如下的自同构: 它在 U_1 上为恒等映射, 而在 V_1 上为 σ_2, 则 σ 即有所需性质.

系 非退化二次模的两个同构的子空间有同构的正交补.

证 两个子空间之间的同构可以扩充成该模的自同构, 然后将它限制在它们的正交补上即可.

1.6. 转述

设 $f(x)=\sum_{i=1}^{n}a_{ii}X_i^2+2\sum_{i<j}a_{ij}X_iX_j$ 是 k 上 n 个变量的二次型. 当 $i>j$ 时, 我们令 $a_{ij}=a_{ji}$, 于是 $A=(a_{ij})$ 是对称矩阵. (k^n, f) 叫作与 f (或者与矩阵 A) 相结合的二次模.

定义 7 两个二次型 f 和 f' 称作是等价的, 如果它们所对应的二次模同构.

这时我们记为 $f\sim f'$. 如果 A 和 A' 是 f 和 f' 的矩阵, 那么这也相当于说存在一个可逆矩阵 X, 使得 $A'=XA{}^tX$ (见 §1.1).

令 $f(X_1, \cdots, X_n)$ 和 $g(X_1, \cdots, X_m)$ 是两个二次型. 我们以 $f\dot{+}g$ (或者在不混淆时写成 $f+g$) 表示 $(n+m)$ 个变量的二次型

$$f(X_1, \cdots, X_m)+g(X_{n+1}, \cdots, X_{n+m}).$$

这个运算对应于直和运算(见 § 1.2 定义 2). 类似地, 我们把 $f\dot{+}(-g)$ 写成 $f\dot{-}g$(或简写成 $f-g$). 这里有一些转述的例子.

定义 4′ 两变量二次型 $f(X_1, X_2)$ 称作是双曲的二次型, 如果我们有

$$f\sim X_1X_2\sim X_1^2-X_2^2.$$

(这意味着对应的二次模 (k^2, f) 是双曲平面, 见定义 4.)

我们称二次型 $f(X_1, \cdots, X_n)$ 表示元素 $a\in k$, 如果存在 $x\in k^n$, $x\neq 0$, 使 $f(x)=a$. 特别地, f 表示 $0\Leftrightarrow$ 对应的二次模包有非零迷向元素.

命题 3′ 如果 f 非退化并且表示 0, 则 $f\sim f_2\dot{+}g$, 其中 f_2 是双曲的. 而且 f 表示 k 中所有元素.

这是命题 3 及其系的转述.

系 1 设 $g=g(X_1, \cdots, X_{n-1})$ 是非退化二次型而 $a\in k^*$, 则下列诸性质彼此等价:

(i) g 表示 a.

(ii) $g\sim h\dot{+}aZ^2$, 其中 h 是 $n-2$ 个变量的二次型.

(iii) 二次型 $f=g\dot{-}aZ^2$ 表示 0.

证 显然(ii)⇒(i). 反之, 如果 g 表示 a, 则对应于 g 的二次模 V 包含元素 x, 使 $x\cdot x=a$. 如果以 H 表示 x 的正交补, 我们有 $V=H\hat{\oplus}kx$, 于是 $g\sim h\dot{+}aZ^2$, 其中 h 表示对于 H 的一组基的二次型.

(ii)⇒(iii) 也可立即得到. 最后, 如果型 $f=g\dot{-}aZ^2$ 有非平凡零点 $(x_1, \cdots, x_{n-1}, z)$, 则或者 $z=0$, 这时 g 表示 0, 因此

也表示 a; 或者 $z\neq 0$, 这时 $g(x_1/z, \cdots, x_{n-1}/z)=a$. 于是(iii)$\Rightarrow$(i).

系 2 设 g 和 h 是秩$\geqslant 1$ 的两个非退化型, 令 $f=g\dotplus h$. 则下列诸性质彼此等价:

(a) f 表示 0.

(b) 存在 $a\in k^*$, 使 g 和 h 均表示 a.

(c) 存在 $a\in k^*$, 使 $g\dotplus -aZ^2$ 和 $h\dotplus -aZ^2$ 均表示 0.

证 由系 1 即得到等价关系(b)$\Leftrightarrow$(c). 推理(b)$\Rightarrow$(a)是显然的. 现在让我们证明(a)$\Rightarrow$(b): f 的非平凡零点可以写成形式(x, y), 使 $g(x)=h(y)$. 如果元素 $a=g(x)=h(y)$不为 0, 显然(b)成立. 如果 $a=0$, 则型 h 和 g 必有一个表示 0. 例如设 g 表示 0, 则 g 可表示 k 中每个元素. 特别地, g 可以表示 h 所取的每个非零值.

定理 1 转述成二次型分解成平方和的经典定理:

定理 1′ 设 f 为 n 变量二次型, 则存在 $a_1, \cdots, a_n\in k$, 使 $f\sim a_1X_1^2+\cdots+a_nX_n^2$.

f 的秩是 $a_i\neq 0$ 的下标 i 的个数. f 的秩等于 $n\Leftrightarrow f$ 的判别式 $a_1a_2\cdots a_n\neq 0$(即 f 非退化).

最后, Witt 定理的系可转述成下面的"消去定理":

定理 4 设 $f=g\dotplus h$, $f'=g'\dotplus h'$ 是两个非退化二次型. 如果$f\sim f'$ 并且 $g\sim g'$, 则 $h\sim h'$.

系 如果 f 非退化, 则

$$f\sim g_1\dotplus\cdots\dotplus g_m\dotplus h,$$

其中 $g_1, \cdots, g_m$ 是双曲的, 而 h 不表示 0. 这个分解不计等价是唯一的.

证 存在性由命题 3′ 推出, 而唯一性由定理 4 推出.

[双曲因子的个数 m 可以刻划成由 f 定义的二次模的极

大迷向子空间的维数.]

1.7. $\mathbf{F}_q$ 上二次型

设 $p\neq 2$ 为素数，$q=p^f$ 为 p 之方幂，$\mathbf{F}_q$ 为 q 元域(见第一章§1).

命题 4 秩$\geqslant 2$ ($\geqslant 3$)的 $\mathbf{F}_q$ 上二次型表示 $\mathbf{F}_q^*(\mathbf{F}_q)$ 中所有元素.

证 根据命题 3 的系 1，只需证明 3 变量的二次型表示 0，而这作为 Chevalley 定理的推论在第一章§2 中已经证明过了.

[让我们指明不用 Chevalley 定理怎样证明这个定理. 我们必需证明，如果 $a, b, c\in\mathbf{F}_q$，则方程

$$ax^2+by^2=c \tag{*}$$

有解. 设 $A=\{ax^2|x\in\mathbf{F}_q\}$，$B=\{c-by^2|y\in\mathbf{F}_q\}$. 易知 A 和 B 均有 $(q+1)/2$ 个元素. 于是 $A\cap B\neq\emptyset$，从而给出(*)的一组解.]

现在让我们注意 $\mathbf{F}_q^*/\mathbf{F}_q^{*2}$ 只有两个元素(第一章§3.1). 命 $a\in\mathbf{F}_q^*$ 是一个非平方元素.

命题 5 $\mathbf{F}_q$ 上秩 n 的每个非退化二次型等价于:

$$X_1^2+\cdots+X_{n-1}^2+X_n^2 \quad 或者 \quad X_1^2+\cdots+X_{n-1}^2+aX_n^2,$$

按照其判别式是否为平方元素而定.

证 $n=1$ 时这是显然的. 如果 $n\geqslant 2$，由命题 4 知型 f 表示 1，因此它等价于 X_1^2+g，其中 g 是 $n-1$ 个变量的型，然后对 g 利用归纳假设即可.

系 $\mathbf{F}_q$ 上两个非退化二次型等价的充要条件是它们有同样的秩和同样的判别式.

(当然判别式看成是商群 $\mathbf{F}_q^*/\mathbf{F}_q^{*2}$ 中元素.)

§2. $\mathbf{Q}_p$ 上的二次型

在本节中(§2.4 除外) p 是素数而 k 为 p-adic 域 $\mathbf{Q}_p$. 所有的二次模均是 k 上的非退化的. 对于二次型我们也作同样的规定.

2.1. 两个不变量

设 (V, Q) 是秩 n 的二次模, $d(Q)$ 是它的判别式(它是 k^*/k^{*2} 中元素, 见 §1.1). 如果 $\boldsymbol{e}=(e_1, \cdots, e_n)$ 是 V 的正交基并且令 $a_i=e_i\cdot e_i$, 便有

$$d(Q)=a_1\cdots a_n \quad (\in k^*/k^{*2}).$$

(下面我们常常将 k^* 中一元素和它 $\bmod k^{*2}$ 之同余类用同一字母表示.)

现在让我们回忆一下, 如果 $a, b\in k^*$, 我们在第三章 §1.1 中定义了 Hilbert 符号 $(a, b)=\pm1$. 令

$$\varepsilon(\boldsymbol{e})=\prod_{i<j}(a_i, a_j).$$

于是有 $\varepsilon(\boldsymbol{e})=\pm1$. 而且 $\varepsilon(\boldsymbol{e})$ 是 (V, Q) 的不变量:

定理 5 数 $\varepsilon(\boldsymbol{e})$ 与正交基 $\boldsymbol{e}$ 的选取无关.

证 如果 $n=1$, 则 $\varepsilon(\boldsymbol{e})=1$. 如果 $n=2$, 则 $\varepsilon(\boldsymbol{e})=1\Leftrightarrow$ 型 $Z^2-a_1X^2-a_2Y^2$ 表示 0, 这也相当于说 $\Leftrightarrow a_1X^2+a_2Y^2$ 表示 1 (见命题 3′ 的系 1). 但是后一条件意味着存在 $v\in V$ 使 $Q(v)=1$, 而这一点不依赖于 $\boldsymbol{e}$ 的选取. 当 $n\geqslant3$ 时, 我们对 n 用数学归纳法. 根据定理 2, 我们只需证明当 $\boldsymbol{e}$ 和 $\boldsymbol{e}'$ 毗连时有 $\varepsilon(\boldsymbol{e})=\varepsilon(\boldsymbol{e}')$. 由于 Hilbert 符号的对称性, 如果置换 e_i 则不改变 $\varepsilon(\boldsymbol{e})$ 的值. 因此可以假设 $\boldsymbol{e}'=(e_1', \cdots, e_n')$ 使 $e_1=e_1'$. 如果令 $a_i'=e_i'\cdot e_i'$, 则 $a_1'=a_1$. 于是可以将 $\varepsilon(\boldsymbol{e})$ 写成形式

$$\varepsilon(\boldsymbol{e}) = (a_1,\ a_2\cdots a_n) \prod_{2\leqslant i<j} (a_i,\ a_j)$$
$$= (a_1,\ d(Q)a_1) \prod_{2\leqslant i<j} (a_i,\ a_j),$$
这是因为 $$d(Q) = a_1\cdots a_n.$$

类似地，
$$\varepsilon(\boldsymbol{e}') = (a_1,\ d(Q)\,a_1) \prod_{2\leqslant i<j} (a_i',\ a_j').$$
但是将归纳假设用于 e_1 的正交补，则有
$$\prod_{2\leqslant i<j} (a_i,\ a_j) = \prod_{2\leqslant i<j} (a_i',\ a_j'),$$
由此即得所需结果.

从现在起我们把 $\varepsilon(\boldsymbol{e})$ 记成 $\varepsilon(Q)$.

转述 如果 f 是 n 变量二次型而
$$f \sim a_1X_1^2 + \cdots + a_nX_n^2,$$
则两个元素 $$d(f) = a_1\cdots a_n (\in k^*/k^{*2}),$$
$$\varepsilon(f) = \prod_{i<j} (a_i,\ a_j)\ \ (\in\{\pm 1\})$$
是 f 之等价类的不变量.

2.2. 用二次型表示 k 中元素

引理 a) $\mathbf{F}_2$-向量空间 k^*/k^{*2} 中的元素个数为 2^r，其中
$$r = \begin{cases} 2, & \text{如果 } p \neq 2, \\ 3, & \text{如果 } p = 2. \end{cases}$$

b) 如果 $a \in k^*/k^{*2}$ 而 $\varepsilon = \pm 1$，令
$$H_a^\varepsilon = \{x \in k^*/k^{*2} \mid (x,\ a) = \varepsilon\}.$$
当 $a=1$ 时，H_a^1 有 2^r 个元素而 $H_a^{-1} = \emptyset$. 当 $a \neq 1$ 时，H_a^ε 有 2^{r-1} 个元素 $(\varepsilon = \pm 1)$.

c) 设 $a,\ a' \in k^*/k^{*2}$ 而 $\varepsilon,\ \varepsilon' = \pm 1$. 假设 H_a^ε 和 $H_{a'}^{\varepsilon'}$ 均非空. 则 $H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \emptyset \Leftrightarrow a = a'$ 并且 $\varepsilon = -\varepsilon'$.

证 a)在第二章 § 3.3 中业已证明. b)情形 $a=1$ 是显然的. 如果 $a\neq 1$, 同态 $b\mapsto(a, b)$ 将 k^*/k^{*2} 映到$\{\pm 1\}$之上(第三章 § 1.2, 定理 2). 因此其核 H_a^1 是 k/k^{*2} 的超平面, 从而有 2^{r-1} 个元素. 它的补 H_a^{-1} 也有 2^{r-1} 个元素 (这是平行于 H_a^1 的"仿射"超平面). 最后,如果 H_a^ε 和 $H_{a'}^{\varepsilon'}$ 均非空且不交, 则每个集合都必需有 2^{r-1} 个元素并且彼此互为补集. 这就导致 $H_a^1=H_{a'}^1$, 于是

$$(x,\ a)=(x,\ a') \quad (\text{对每个 } x\in k^*/k^{*2}).$$

由于 Hilbert 符号是非退化的, 于是 $a=a'$ 并且 $\varepsilon=-\varepsilon'$. 反过来是显然的.

现在设 f 为秩 n 的二次型. $d=d(f)$ 和 $\varepsilon=\varepsilon(f)$ 为它的两个不变量.

定理 6 f 表示 0 的充要条件为

i) $n=2$ 而 $d=-1(\in k^*/k^{*2})$.

ii) $n=3$ 而 $(-1,\ -d)=\varepsilon$.

iii) $n=4$; $d\neq 1$ 或者 $d=1$ 而 $\varepsilon=(-1,\ -1)$.

iv) $n\geqslant 5$.

(特别地,变量数$\geqslant 5$的二次型均表示 0.)

在证明此定理之前,我们先指出它的一个推论: 设

$$a\in k^*/k^{*2}, \quad f_a=f\dotplus -aZ^2.$$

我们知道(见 § 1.6), f_a表示 $0\Leftrightarrow f$ 表示 a. 另一方面,容易验证

$$d(f_a)=-ad, \quad \varepsilon(f_a)=(-a,\ d)\varepsilon.$$

将定理 6 用于 f_a 并且考虑到上述二公式就得到:

系 令 $a\in k^*/k^{*2}$. 则 f 表示 a 的充要条件是

i) $n=1$ 而 $a=d$.

ii) $n=2$ 而 $(a,\ -d)=\varepsilon$,

iii) $n=3$; $a\neq -d$ 或者 $a=-d$ 并且 $(-1, -d)=\varepsilon$.

iv) $n\geqslant 4$.

(注意在此及定理 6 的陈述中, a 和 d 看成是 k^*/k^{*2} 中元素, 从而 $a\neq -d$ 是指 a 不等于 $-d$ 与某平方元素之积.)

定理 6 的证明. 我们记 f 为 $f\sim a_1X_1^2+\cdots+a_nX_n^2$ 并且分别考虑 $n=2, 3, 4$ 和 $\geqslant 5$ 诸情形.

i) $n=2$ 情形.

型 f 表示 $0\Leftrightarrow -a_1/a_2$ 是平方元素. 但是在 k^*/k^{*2} 中

$$-a_1/a_2=-a_1a_2=-d.$$

于是这意味着 $d=-1$.

ii) $n=3$ 情形.

型 f 表示 $0\Leftrightarrow$ 型 $-a_3f\sim -a_3a_1X_1^2-a_3a_2X_2^2-X_3^2$ 表示 0. 由 Hilbert 符号的定义本身可知, 后一个二次型表示

$$0\Leftrightarrow(-a_3a_1, -a_3a_2)=1.$$

将其展开, 我们发现

$$(-1, -1)(-1, a_1)(-1, a_2)(a_3, a_3)(a_1, a_2)(a_1, a_3)(a_2, a_3)=1.$$

但是 $(a_3, a_3)=(-1, a_3)$ (见第三章 § 1.1, 命题 2, 公式 iv). 因此上述条件就可重新写成如下形式:

$$(-1, -1)(-1, a_1a_2a_3)(a_1, a_2)(a_1, a_3)(a_2, a_3)=1.$$

这就是 $(-1, -d)\varepsilon=1$, 也就是 $(-1, -d)=\varepsilon$.

iii) $n=4$ 情形.

根据命题 3′ 的系 2, f 表示 $0\Leftrightarrow$ 存在元素 $x\in k^*/k^{*2}$, 使它可由型 $a_1X_1^2+a_2X_2^2$ 及 $-a_3X_3^2-a_4X_4^2$ 表示. 根据上面系的 ii), 这样的 x 可以刻划为

$$(x, -a_1a_2)=(a_1, a_2),$$

并且
$$(x, -a_3a_4)=(-a_3, -a_4).$$

设 A 为第一条件定义的 k^*/k^{*2} 之子集, B 是由第二条件定义的 k^*/k^{*2} 之子集. 于是 f 不表示 $0 \Leftrightarrow A\cap B=\emptyset$. 现在 A 和 B 显然非空(例如 $a_1\in A$, $-a_3\in B$). 如本小节一开始所述引理的 c) 部分可知, 关系 $A\cap B=\emptyset$ 等价于

$$a_1a_2=a_3a_4 \quad \text{和} \quad (a_1, a_2)=-(-a_3, -a_4).$$

第一个条件意味着 $d=1$. 如果它成立, 则

$$\varepsilon=(a_1, a_2)(a_3, a_4)(a_3a_4, a_3a_4).$$

使用关系 $(x, x)=(-1, x)$ (第三章 § 1.1, 命题 2 的公式 iv)), 由此便给出

$$\begin{aligned}\varepsilon&=(a_1, a_2)(a_3, a_4)(-1, a_3a_4)\\&=(a_1, a_2)(-a_3, -a_4)(-1, -1).\end{aligned}$$

于是第二条件可以写成 $\varepsilon=-(-1, -1)$. 由此即得结果.

iv) $n\geqslant 5$ 情形.

只需讨论 $n=5$ 情形. 利用上述引理和上述系的 ii) 部分我们看出, 秩 2 的型至少表示 k^*/k^{*2} 中 2^{r-1} 个元素, 由此得出这对于秩 $\geqslant 2$ 的型也同样正确. 因为 $2^{r-1}\geqslant 2$, 从而 f 至少还表示 k^*/k^{*2} 中与 d 不同的一个元素 a. 我们有

$$f\sim aX^2\dotplus g,$$

这里 g 为秩 4 的型. g 的判别式等于 d/a, 从而不是 1. 而由 iii) 可知 g 表示 0, 从而这对于 f 同样正确, 于是完成了定理 6 的证明.

注 1) 设 f 是不表示 0 的二次型. 上面的结果表明, 可以被 f 所表示的 k^*/k^{*2} 中之数当 $n=1, 2, 3, 4$ 时分别为 1, 2^{r-1}, 2^r-1, 2^r.

2) 我们已经看到, 任一 $\mathbf{Q}_p$ 上 5 变量二次型均可表示 0. 与此相联系, 让我们提一下 E. Artin 的一个猜想: $\mathbf{Q}_p$ 上的 $\geqslant d^2+1$ 个变量的 d 次齐次多项式必有非平凡零点. 当 $d=3$

时已经被肯定地加以解决(例如见 T. Springer, Koninkl. Nederl. Akad. van Wetenss., 1955, pp. 512～516). 在大约三十年里,未能解决一般情形. 一直到 1966 年, G. Terjanian 证明了 Artin 猜想是不对的: $\mathbf{Q}_2$ 上存在着 18 个变量的 4 次齐次多项式,它没有非平凡零点. Terjanian 从多项式

$$n(X, Y, Z)=X^2YZ+Y^2ZX+Z^2XY+X^2Y^2+Y^2Z^2+Z^2X^2-X^4-Y^4-Z^4$$

出发,该多项式有性质:如果(x, y, z)是$(\mathbf{Z}_2)^3$中本原向量,则$n(x, y, z)\equiv -1 \pmod 4$. 令

$$f(X_1, \cdots, X_9)=n(X_1, X_2, X_3)+n(X_4, X_5, X_6)+n(X_7, X_8, X_9).$$

我们有:如果$(x_1, \cdots, x_9)$本原, 则$f(x_1, \cdots, x_9)\not\equiv 0 \pmod 4$. 由此容易推出多项式

$$F(X_1, \cdots, X_{18})=f(X_1, \cdots, X_9)+4f(X_{10}, \cdots, X_{18})$$

没有非平凡零点. (对于所有的 $\mathbf{Q}_p$ 均存在类似的例子, 但是次数更高.)

尽管如此, 我们知道 Artin 猜想"几乎"是对的: 对每个固定的次数 d, Artin 猜想对于除了有限个之外的全部素数 p 都是对的(Ax-Kochen, Amer. J. of Math., 1965). 但是甚至对于 $d=4$, 我们也还都不知道如何决定例外素数集合.

2.3. 分类

定理 7 k 上的两个二次型等价 $\Leftrightarrow$ 它们有同样的秩, 同样的判别式和不变量 ε.

证 由定义即知两个等价的二次型有同样的不变量. 反过来,我们对所考虑的两个型 f 和 g 的次数 n 进行归纳($n=0$

的情形是显然的). 根据定理 6 的系, f 和 g 表示 k^*/k^{*2} 中同样元素. 因此可以求得 $a\in k^*$, 使它同时被 f 和 g 表示. 这使我们可以写成:

$$f\sim aZ^2+f', \quad g\sim aZ^2+g',$$

其中 f' 和 g' 是秩 $n-1$ 的二次型. 于是有

$$d(f')=ad(f)=ad(g)=d(g'),$$
$$\varepsilon(f')=\varepsilon(f)(a,\ d(f'))=\varepsilon(g)(a,\ d(g'))=\varepsilon(g'),$$

从而 f' 和 g' 有同样的不变量. 根据归纳假设我们有 $f'\sim g'$, 于是 $f\sim g$.

系 不计等价, 只存在唯一的一个秩 4 的二次型不表示 0. 如果 $(a, b)=-1$, 则这个型是 $z^2-ax^2-by^2+abt^2$.

证 事实上, 根据定理 6, 这样的二次型可以用

$$d(f)=1, \quad \varepsilon(f)=-(-1,\ -1)$$

来刻划. 经简单计算可知 $z^2-ax^2-by^2+abt^2$ 有这些性质.

注 这个型是 $\mathbf{Q}_p$ 上唯一的 4 次体的标准范. 这个体可以定义成以 $\{1, i, j, k\}$ 为基的"四元数"体, 其中

$$i^2=a, \quad j^2=b, \quad ij=k=-ji,$$

而

$$(a,\ b)=-1.$$

命题 6 设 $n\geqslant 1$, $d\in k^*/k^{*2}$ 而 $\varepsilon=\pm 1$. 则存在秩 n 二次型 f 使 $d(f)=d$, $\varepsilon(f)=\varepsilon$ 的充要条件是 $n=1$, $\varepsilon=1$; 或者 $n=2$, $d\neq -1$; 或者 $n=2$, $\varepsilon=1$; 或者 $n\geqslant 3$.

证 $n=1$ 情形是显然的. 如果 $n=2$, 则有 $f\sim aX^2+bY^2$, 而且若 $d(f)=-1$, 则 $\varepsilon(f)=(a,\ b)=(a,\ -ab)=1$. 因此我们不能同时有 $d(f)=-1$ 和 $\varepsilon(f)=-1$. 反过来, 如果 $d=-1$, $\varepsilon=1$, 我们取 $f=X^2-Y^2$; 如果 $d\neq -1$, 则存在 $a\in k^*$ 使 $(a,\ -d)=\varepsilon$, 我们取 $f=aX^2+adY^2$.

如果 $n=3$, 我们取 $a\in k^*/k^{*2}$, $a\neq -d$. 根据上面所看到

的，存在一个秩 2 的型 g，使得 $d(g)=ad$，$\varepsilon(g)=\varepsilon(a, -d)$. 于是型 aZ^2+g 即为所求. 对于 $n\geqslant 4$ 的情形，取

$$f=g(X_1, X_2, X_3)+X_4^2+\cdots+X_n^2$$

便可化成 $n=3$ 的情形，其中 g 有所需要的不变量.

系 以 N 表示 $\mathbf{Q}_p$ 上秩 n 二次型的类数，则

$$N=\begin{cases} 4, & \text{如果 } n=1,\ p\neq 2; \\ 8, & \text{如果 } n=1,\ p=2; \\ 7, & \text{如果 } n=2,\ p\neq 2; \\ 15, & \text{如果 } n=2,\ p=2; \\ 8, & \text{如果 } n\geqslant 3,\ p\neq 2; \\ 16, & \text{如果 } n\geqslant 3,\ p=2. \end{cases}$$

证 事实上当 $p\neq 2$ 时 $d(f)$ 可以取 4 个值，当 $p=2$ 时，$d(f)$ 可以取 8 个值. 而 $\varepsilon(f)$ 可以取 2 个值.

2.4. 实数域情形

设 f 为实数域 $\mathbf{R}$ 上秩 n 二次型. 我们知道

$$f\sim X_1^2+\cdots+X_r^2-Y_1^2-\cdots-Y_s^2,$$

其中 r 和 s 是非负整数并且 $r+s=n$. (r, s) 只依赖于 f，叫作 f 的符号量. 如果 r 或 $s=0$，即如果 f 不变符号我们称 f 为定二次型；否则便称 f 为不定二次型（这即是 f 表示 0 的情形）.

象情形 $\mathbf{Q}_p$ 那样定义不变量 $\varepsilon(f)$. 由于

$$(-1, -1)=-1,$$

我们有

$$\varepsilon(f)=(-1)^{\frac{s(s-1)}{2}}=\begin{cases} 1, & \text{如果 } s\equiv 0,\ 1 \pmod 4), \\ -1, & \text{如果 } s\equiv 2,\ 3 \pmod 4). \end{cases}$$

而且

$$d(f)=(-1)^s=\begin{cases}1, & \text{如果 } s\equiv 0 \pmod 2),\\ -1, & \text{如果 } s\equiv 1 \pmod 2).\end{cases}$$

我们看到，$d(f)$和$\varepsilon(f)$的知识由s的$\bmod 4$同余类所决定。特别地，如果$n\leqslant 3$，则$d(f)$和$\varepsilon(f)$决定了f的等价类。

还可以检查定理6的前三部分及其系对于$\mathbf{R}$是正确的（事实上，它们的证明只使用了Hilbert符号的非退化性，而这一点也可以用于$\mathbf{R}$）。显然第iv）部分是不能推广的。

§3. Q上的二次型

下面所考虑的二次型的系数均属于$\mathbf{Q}$并且是非退化的。

3.1. 型的不变量

象第三章§2那样，我们以V表示所有素数与符号∞组成的集合，令$\mathbf{Q}_\infty=\mathbf{R}$。

设$f\sim a_1X_1^2+\cdots+a_nX_n^2$是秩$n$二次型。我们把它与如下一些不变量相联系：

a）判别式$d(f)=a_1\cdots a_n\in\mathbf{Q}^*/\mathbf{Q}^{*2}$。

b）设$v\in V$，单射$\mathbf{Q}\to\mathbf{Q}_v$可使我们将$f$看成是$\mathbf{Q}_v$上的二次型（我们将把它记成$f_v$）。$f_v$的不变量记成$d_v(f)$和$\varepsilon_v(f)$。显然$d_v(f)$是$d(f)$在自然映射$\mathbf{Q}^*/\mathbf{Q}^{*2}\to\mathbf{Q}_v^*/\mathbf{Q}_v^{*2}$之下的象。我们有

$$\varepsilon_v(f)=\prod_{i<j}(a_i,\ a_j)_v.$$

乘积公式（第三章§2.1.定理3）给出关系

$$\prod_{v\in V}\varepsilon_v(f)=1.$$

c）实二次型f的符号量$(r,\ s)$是f的又一个不变量。

有时把不变量$d_v(f)$，$\varepsilon_v(f)$和$(r,\ s)$叫作f的局部不变量组。

3.2. 用型表示数

定理 8(Hasse-Minkowski) f 表示 0 的充要条件是对于每个 $v\in V$, 型 f_v 均表示 0.

(换句话说, f 有“整体”零点的充要条件是 f 处处有“局部”零点.)

证 必要性是显然的. 为了证明充分性, 我们把 f 写成如下的形式:

$$f=a_1X_1^2+\cdots+a_nX_n^2,\quad a_i\in\mathbf{Q}^*.$$

把 f 改成 a_1f, 还可以假设 $a_1=1$. 我们分别考虑情形 $n=2$, 3, 4 和 $\geqslant 5$:

i) 情形 $n=2$.

我们有 $f=X_1^2-aX_2^2$. 由于 f_∞ 表示 0, 从而 $a>0$. 如果将 a 写成

$$a=\prod_p p^{v_p(a)},$$

则 f_p 表示 0 这一事实说明 a 为 $\mathbf{Q}_p$ 中平方元素, 于是 $v_p(a)$ 为偶数. 由此推出 a 是 $\mathbf{Q}$ 中平方元素, 从而 f 表示 0.

ii) 情形 $n=3$(Legendre).

我们有 $f=X_1^2-aX_2^2-bX_3^2$. 由于 a 和 b 均允许乘一个平方因子, 我们可设 a, b 均是无平方因子的整数 (即对每个素数 p, $v_p(a)$ 和 $v_p(b)$ 均是 0 或 1). 还可以假设 $|a|\leqslant|b|$. 现在对整数 $m=|a|+|b|$ 用数学归纳法. 如果 $m=2$, 我们有

$$f=X_1^2\pm X_2^2\pm X_3^2.$$

因为 f_∞ 必须表示 0, 情形 $X_1^2+X_2^2+X_3^2$ 被排除掉. 而在其余情形下, f 均表示 0.

现在设 $m>2$, 即 $|b|\geqslant 2$, 将 b 写成

$$b=\pm p_1\cdots p_k,$$

其中 p_i 为两两不同的素数. 设 p 为 p_i 中的某一个, 我们将证

明 a 是 $\bmod p$ 平方元素．如果 $a\equiv 0 \pmod p$，这是显然的．否则 a 是 p-adic 单位．根据假设，存在 $(x, y, z)\in(\mathbf{Q}_p)^3$，使

$$z^2-ax^2-by^2=0.$$

可以假设 (x, y, z) 本原（见第二章 § 2.1，命题 6）．我们有

$$z^2-ax^2\equiv 0 \pmod p.$$

由此可见，如果 $x\equiv 0 \pmod p$，则 $z\equiv 0 \pmod p$，于是 $p^2\mid by^2$．由于 $v_p(b)=1$，从而 $y\equiv 0 \pmod p$，这就与 (x, y, z) 本原这一事实相矛盾．于是我们有 $x\not\equiv 0 \pmod p$，这表明 a 是 $(\bmod p)$ 平方元素． 现在因为 $\mathbf{Z}/b\mathbf{Z}=\prod \mathbf{Z}/p_i\mathbf{Z}$，我们看到 a 是 $\bmod b$ 平方元素．因此存在整数 t 和 b'，使

$$t^2=a+bb'.$$

我们还可以取 t 使 $|t|\leqslant|b|/2$． 公式 $bb'=t^2-a$ 表明 bb' 是扩张 $k(\sqrt{a})/k$ 的范，其中 $k=\mathbf{Q}$ 或 $\mathbf{Q}_v$． 由此我们推出（论据同第三章命题 1），f 在 k 中表示 0 的充要条件为

$$f'=X_1^2-aX_2^2-b'X_3^2$$

表示 0．特别地，在每个 $\mathbf{Q}_v$ 中 f' 表示 0．但是我们有

$$|b'|=\left|\frac{t^2-a}{b}\right|\leqslant\frac{|b|}{4}+1<|b| \quad (\text{因为} |b|\geqslant 2).$$

记 $b'=b''u^2$，其中 b''，u 为整数而 b'' 无平方因子．从而有 $|b''|<|b|$．将归纳假设用于型 $f''=X_1^2-aX_2^2-b''X_3^2$，由于它等价于 f'，从而它在 $\mathbf{Q}$ 中表示 0，因此 f 在 $\mathbf{Q}$ 中也表示 0．

iii) 情形 $n=4$．

记 $f=aX_1^2+bX_2^2-(cX_3^2+dX_4^2)$．令 $v\in V$．由于 f_v 表示 0，根据 § 1.6，命题 3′ 的系 2 可知存在 $x_v\in\mathbf{Q}_v^*$，使 x_v 同时被 $aX_1^2+bX_2^2$ 和 $cX_3^2+dX_4^2$ 所表示．由定理 6 系的 ii) 部分（它同样可以用于 $\mathbf{Q}_\infty=\mathbf{R}$），这等价于说

$$(x_v,\ -ab)_v=(a,\ b)_v,\quad (x_v,\ -cd)_v=(c,\ d)_v$$
(对于每个 $v\in V$).

由于
$$\prod_{v\in V}(a,\ b)_v=\prod_{v\in V}(c,\ d)_v=1,$$
我们可以应用第三章 §2.2 的定理 4, 由此可知存在 $x\in \mathbf{Q}^*$, 使
$$(x,\ -ab)_v=(a,\ b)_v,\quad (x,\ -cd)_v=(c,\ d)_v$$
(对每个 $v\in V$).

在每个 $\mathbf{Q}_v$ 中型 $aX_1^2+bX_2^2-xZ^2$ 表示 0, 从而由上可知它在 $\mathbf{Q}$ 中也表示 0. 于是 x 在 $\mathbf{Q}$ 中可以被 $aX_1^2+bX_2^2$ 所表示, 同样的推理可用于 $cX_3^2+dX_4^2$, 由此即知 f 表示 0.

iv) 情形 $n\geqslant 5$.

对 n 归纳. 将 f 记为
$$f=h\dot{-}g,$$
其中 $h=a_1X_1^2+a_2X_2^2$, $g=-(a_3X_3^2+\cdots+a_nX_n^2)$.

令 S 为 V 的子集, 由 ∞, 2 以及
$$\{p\in V\mid 存在某个\ i\geqslant 3,\ 使\ v_p(a_i)\neq 0\}$$
所组成. 这是有限集. 令 $v\in S$. 由于 f_v 表示 0, 从而存在 $a_v\in \mathbf{Q}_v^*$, 它在 $\mathbf{Q}_v$ 中同时被 h 和 g 所表示. 于是存在
$$x_i^v\in \mathbf{Q}_v\quad (1\leqslant i\leqslant n),$$
使得
$$h(x_1^v,\ x_2^v)=a_v=g(x_3^v,\ \cdots,\ x_n^v).$$
但是 $\mathbf{Q}_v^*$ 的平方元素形成开集(见第二章 §3.3). 应用逼近定理(第三章 §2.2 引理 2), 可知存在 x_1, $x_2\in \mathbf{Q}$, 使得令
$$a=h(x_1,\ x_2),$$
便有 $a/a_v\in \mathbf{Q}_v^{*2}$ (对于每个 $v\in S$). 现在考虑型 $f_1=aZ^2\dot{-}g$. 如果 $v\in S$, g 在 $\mathbf{Q}_v$ 中表示 a_v, 由于 $a/a_v\in \mathbf{Q}_v^{*2}$, 从而它也表示 a, 于是 f_1 在 $\mathbf{Q}_v$ 中表示 0. 如果 $v\notin S$, g 之系数 $-a_3$, $\cdots$, $-a_n$ 均是 v-adic 单位, 因此 $d_v(g)$ 也是 v-adic 单位. 而由于

$v \neq 2$, 我们有 $\varepsilon_v(g)=1$(这也可以由第二章 § 2.2 的定理 1 系 2 以及 Chevalley 定理而推出). 在所有情形下, f_1 在 $\mathbf{Q}_v$ 中均表示 0. 由于 f_1 的秩为 $n-1$, 利用归纳假设可知 f_1 在 $\mathbf{Q}$ 中表示 0, 即 g 在 $\mathbf{Q}$ 中表示 a. 由于 h 表示 a, 从而 f 表示 0, 这就完成了定理的证明.

系 1 设 $a \in \mathbf{Q}^*$. 则 f 在 $\mathbf{Q}$ 中表示 a 的充要条件是它在每个 $\mathbf{Q}_v$ 中均表示 a.

证 将定理用于型 $aZ^2 \dot{-} f$ 即可.

系 2(Meyer) 秩 $\geqslant 5$ 的二次型表示 0 的充要条件是它为不定二次型(即它在 $\mathbf{R}$ 中表示 0).

证 因为由定理 6, 这样的二次型在每个 $\mathbf{Q}_p$ 中均表示 0.

系 3 令 n 为 f 的秩. 假设 $n=3$(或者 $n=4$ 而 $d(f)=1$), 如果除了至多一个之外 f 在所有 $\mathbf{Q}_v$ 中均表示 0, 则 f 表示 0.

证 假设 $n=3$. 按照定理 6, f 在 $\mathbf{Q}_p$ 中表示 0 的充要条件是

$$(*)_v \qquad (-1,\ -d(f))_v = \varepsilon_v(f).$$

但是两组 $\varepsilon_v(f)$ 和 $(-1,\ -d(f))_v$ 均满足第三章 § 2.1 的乘积公式. 由此可知, 如果 $(*)_v$ 对于除了至多一个之外的全部 v 均成立, 那末 $(*)_v$ 对于全部 v 均成立. 由定理 8 即知 f 表示 0.

当 $n=4$ 并且 $d(f)=1$ 时可以同样推理, 只不过是将等式 $(*)_v$ 改成 $(-1,\ -1)_v=\varepsilon_v(f)$ 罢了.

注 1) 假设 $n=2$, 而 f 在除了有限个之外的全部 $\mathbf{Q}_v$ 中均表示 0. 利用算术级数中的素数定理(第四章 § 4.3)可以证明 f 表示 0.

2) 定理 8 不能推广到次数 $\geqslant 3$ 的齐次多项式去. 例如 Selmer 证明了, 方程

$$3X^3+4Y^3+5Z^3=0$$

在每个 $\mathbf{Q}_v$ 中均有非平凡解，但是在 $\mathbf{Q}$ 中则不然.

3.3. 分类

定理 9 设 f 和 f' 是 $\mathbf{Q}$ 上的两个二次型. 则 f 和 f' 在 $\mathbf{Q}$ 上等价的充要条件是它们在每个 $\mathbf{Q}_v$ 上等价.

证 必要性显然. 为证充分性, 我们对 f 和 f' 的秩 n 归纳. 如果 $n=0$, 则没有什么可证的. 否则的话, 存在 $a\in\mathbf{Q}^*$ 可被 f 所表示, 从而也可被 f' 所表示(定理 8 的系 1). 因此我们有 $f\sim aZ^2\dotplus g$, $f'\sim aZ^2\dotplus g'$. 根据 § 1.6 的定理 4, 我们对所有的 $v\in V$, 在 $\mathbf{Q}_v$ 上均有 $g\sim g'$. 由归纳假设可知在 $\mathbf{Q}$ 上 $g\sim g'$, 从而 $f\sim f'$.

系 设 (r, s) 和 (r', s') 是 f 和 f' 的符号量. 则 f 和 f' 等价的充要条件是:

$$d(f)=d(f'),\ (r, s)=(r', s')$$

并且对每个 $v\in V$ 均有 $\quad \varepsilon_v(f)=\varepsilon_v(f')$.

证 事实上, 这些条件意味着 f 和 f' 在每个 $\mathbf{Q}_v$ 上均等价.

注 不变量组 $d=d(f)$, $\varepsilon_v=\varepsilon_v(f)$ 和 (r, s) 不是随意的, 它们要满足如下一些关系:

(1) 对几乎所有的 $v\in V$, $\varepsilon_v=1$, 并且 $\prod_{v\in V}\varepsilon_v=1$.

(2) 当 $n=1$ 或者 $n=2$ 而 d 在 $\mathbf{Q}_v^*/\mathbf{Q}_v^{*2}$ 中之象 $d_v=-1$ 时, 有 $\varepsilon_v=1$.

(3) $r, s\geqslant 0$ 而且 $r+s=n$.

(4) $d_\infty=(-1)^s$.

(5) $\varepsilon_\infty=(-1)^{\frac{s(s-1)}{2}}$.

反之:

命题 7 设 d, $(\varepsilon_v)_{v\in V}$ 和 (r, s) 满足上述关系(1)~(5), 则存在 $\mathbf{Q}$ 上秩 n 二次型具有不变量组 d, $(\varepsilon_v)_{v\in V}$ 和 (r, s).

证 $n=1$ 时显然.

假设 $n=2$. 令 $v\in V$. 由 Hilbert 符号的非退化性以及条件(2), 可证存在 $x_v\in\mathbf{Q}_v^*$ 使 $(x_v, -d)_v=\varepsilon_v$. 由此及条件(1)即知存在 $x\in\mathbf{Q}^*$, 使对每个 $v\in V$ 均有 $(x, -d)_v=\varepsilon_v$ (第三章 §2.2 定理 4). 型 xX^2+xdY^2 即为所求.

假设 $n=3$. 令

$$S=\{v\in V \mid (-d, -1)_v=-\varepsilon_v\}.$$

这是有限集. 如果 $v\in S$, 在 $\mathbf{Q}_v^*/\mathbf{Q}_v^{*2}$ 中取一个元素 c_v 不等于 $-d$ 在此群中之象 $-d_v$. 利用逼近定理(第三章 §2.2 引理 2), 我们看到存在 $c\in\mathbf{Q}^*$, 使对于每个 $v\in S$, c 在 $\mathbf{Q}_v^*/\mathbf{Q}_v^{*2}$ 中之象是 c_v. 由上面所证即知存在秩 2 的型 g 使

$$d(g)=cd, \quad \varepsilon_v(g)=(c, -1)_v\varepsilon_v \quad (\text{对每个 } v\in V).$$

型 $f=cZ^2\dotplus g$ 即为所求. [注意若 $n\leqslant 3$, 我们不需要考虑型的符号量, 因为条件(3), (4), (5)可推得它是 d_∞ 和 ε_∞ 的函数.]

当 $n\geqslant 4$ 时我们对 n 归纳. 先设 $r\geqslant 1$, 利用归纳假设我们得到秩 $n-1$ 的二次型 g, 它有不变量组 d, $(\varepsilon_v)_{v\in V}$ 和 $(r-1, s)$, 型 $X^2\dotplus g$ 即为所求. 当 $r=0$ 时, 我们使用不变量组为 $-d$, $\varepsilon_v(-1, -d)_v$ 和 $(0, n-1)$ 的一个秩 $n-1$ 二次型 h, 型 $-X^2\dotplus h$ 即为所求.

附录 三个平方数的和

设 n 和 p 为正整数. 我们称 n 是 p 个平方数的和, 如果 n 在环 $\mathbf{Z}$ 上可用二次型 $X_1^2+\cdots+X_p^2$ 表示, 即如果存在整数 $n_1, \cdots, n_p$, 使

$$n=n_1^2+\cdots+n_p^2.$$

定理(Gauss)　一个正整数是三个平方数的和的充要条件是它不能表示成 $4^a(8b-1)$，其中 $a,\ b\in\mathbf{Z}$.

(例如若 $4\nmid n$,则 n 是三个平方数的和 $\Leftrightarrow n\equiv 1,\ 2,\ 3,\ 5,\ 6 \pmod 8$.)

证　可设 $n\neq 0$. 条件"n 有形式 $4^a(8b-1)$"等价于说 $-n$ 是 $\mathbf{Q}_2^*$ 中平方元素(第二章 § 3.3 定理 4). 但是我们有

引理 A　设 $a\in\mathbf{Q}^*$,则 a 在 $\mathbf{Q}$ 中可以表示成 $f=X_1^2+X_2^2+X_3^2$ 的充要条件为 $a>0$, 并且 $-a$ 不是 $\mathbf{Q}_2$ 中平方元素.

证　根据定理 8 的系 1, 我们必须表达出在 $\mathbf{R}$ 和所有 $\mathbf{Q}_p$ 中 f 都可以表示 a 这一事实. $\mathbf{R}$ 的情形给出条件 $a>0$. 另一方面, 局部不变量 $d_p(f)$ 和 $\varepsilon_p(f)$ 等于 1. 如果 $p\neq 2$, 我们有

$$(-1,\ -d_p(f))_p=(-1,\ -1)_p=1=\varepsilon_p(f).$$

因此由定理 6 的系可知在 $\mathbf{Q}_p$ 中 f 可表示 a. 如果 $p=2$, 我们有

$$(-1,\ -d_2(f))_2=-1\neq\varepsilon_2(f).$$

由上述同一个系可知 f 在 $\mathbf{Q}_2$ 中表示 $a\Leftrightarrow$ 在 $\mathbf{Q}_2^*/\mathbf{Q}_2^{*2}$ 中 $a\neq -1\Leftrightarrow -a$ 不是 $\mathbf{Q}_2$ 中平方元素.

现在我们必须从 $\mathbf{Q}$ 中表示过渡到 $\mathbf{Z}$ 中表示. 这使用下述引理:

引理 (Davenport-Cassels)　设 $f(X)=\sum\limits_{i,j=1}^{p}a_{ij}X_iX_j$ 是正定二次型, (a_{ij})为整系数对称矩阵. 我们还假设:

(H)　　对于每个 $x=(x_1,\ \cdots,\ x_p)\in\mathbf{Q}^p$, 均有 $y\in\mathbf{Z}^p$, 使

$$f(x-y)<1.$$

如果 f 在 $\mathbf{Q}$ 中可以表示 $n\in\mathbf{Z}$, 那末 f 在 $\mathbf{Z}$ 中也可以表示 n.

证　如果 $x=(x_1,\ \cdots,\ x_p)$和 $y=(y_1,\ \cdots,\ y_p)$为 $\mathbf{Q}^p$ 中两个元素,以 $x\cdot y$ 表示内积 $\sum a_{ij}x_iy_j$. 于是 $x\cdot x=f(x)$.

设 f 在 $\mathbf{Q}$ 中可表示整数 n. 则存在整数 $t>0$, 使 $t^2n=x\cdot x$, 其中 $x\in\mathbf{Z}^p$. 取这种 t 和 x, 使 t 达到极小值. 我们必需证明 $t=1$.

由假设条件(H),可知存在 $y\in\mathbf{Z}^p$, 使

$$\frac{x}{t}=y+z,\qquad z\cdot z<1.$$

如果 $z\cdot z=0$, 则 $z=0$, 而 $\frac{x}{t}$ 有整系数. 由于 t 的极小性, 可知 $t=1$.

现在假设 $z\cdot z\neq 0$，我们令

$$a=y\cdot y-n,\quad b=2(nt-x\cdot y),\quad t'=at+b,\quad x'=ax+by.$$

则 $a, b, t'\in\mathbf{Z}$，并且

$$x'\cdot x'=a^2x\cdot x+2abx\cdot y+b^2y\cdot y=a^2t^2n+ab(2nt-b)+b^2(n+a)$$
$$=n(a^2t^2+2abt+b^2)=t'^2n.$$

而且

$$tt'=at^2+bt=t^2y\cdot y-nt^2+2nt^2-2tx\cdot y$$
$$=t^2y\cdot y-2tx\cdot y+x\cdot x=(ty-x)\cdot(ty-x)=t^2z\cdot z,$$

于是 $t'=tz\cdot z$. 由于 $0<z\cdot z<1$，我们有 $0<t'<t$. 这就与 t 的极小性相矛盾，从而证明了引理.

为了证明定理，现在只需检查型 $f=X_1^2+X_2^2+X_3^2$ 满足引理条件(H). 但这是显然的：如果 $(x_1, x_2, x_3)\in\mathbf{Q}^3$，我们取 $(y_1, y_2, y_3)\in\mathbf{Z}^3$，使 $|x_i-y_i|\leqslant 1/2(1\leqslant i\leqslant 3)$. 于是有 $\sum(x_i-y_i)^2\leqslant 3/4<1$.

系 1(Lagrange) 每个正整数都是四个平方的和.

证 设 $n>0$ 为整数，记 $n=4^a m$，其中 $4\nmid m$. 如果 $m\equiv 1, 2, 3, 5, 6 \pmod 8$，则 m 是三个平方的和，而 n 亦然. 否则便有 $m\equiv -1\pmod 8$，于是 $m-1$ 便是三个平方的和，这时 m 便是四个平方的和，而 n 亦然.

系 2(Gauss) 每个正整数都是三个三角形数之和.

(所谓"三角形数"即是指形为 $\dfrac{m(m+1)}{2}$ 的数，其中 $m\in\mathbf{Z}$.)

证 设 n 为正整数. 将定理用于 $8n+3$，可知存在整数 x_1, x_2, x_3，使

$$x_1^2+x_2^2+x_3^2=8n+3.$$

于是有

$$x_1^2+x_2^2+x_3^2\equiv 3\pmod 8.$$

但是 $\mathbf{Z}/8\mathbf{Z}$ 中的平方元素只有 0, 1 和 4，从而如果 $\mathbf{Z}/8\mathbf{Z}$ 中三个平方元素之和等于 3，则每项必然都等于 1. 这就表明 x_i 均是奇数，从而可写成 $2m_i+1$，其中 m_i 为整数. 我们有

$$\sum_{i=1}^{3}\frac{m_i(m_i+1)}{2}=\frac{1}{8}\left(\sum_{i=1}^{3}(2m_i+1)^2-3\right)=\frac{1}{8}(8n+3-3)=n.$$

第五章 判别式为 ±1 的整二次型

§1. 预备知识

1.1. 定义

设 $n\geqslant 0$ 为整数, 我们对下面的范畴 S_n 感兴趣:

S_n 的对象 E 是秩 n 的自由交换群 (即同构于 $\mathbf{Z}^n$), 其上有双线性型 $E\times E\to\mathbf{Z}$, 表示成 $(x, y)\mapsto x\cdot y$, 使得

(i) 由型 $x\cdot y$ 定义的 E 到 $\mathrm{Hom}(E, \mathbf{Z})$ 中的同态是同构.

易知这条件等价于下面的条件 (见 Bourbaki, 代数, 第九章, §2, 命题 3):

(ii) 如果 (e_i) 是 E 的一组基而 $a_{ij}=e_i\cdot e_j$, 则矩阵 $A=(a_{ij})$ 的行列式等于 ±1.

两个对象 E, $E'\in S_n$ 的同构用显然的方式加以定义, 这时记成 $E\simeq E'$. 为方便起见还引入 $S=\bigcup\limits_{n=0}^{\infty}S_n$.

如果 $E\in S_n$, 函数 $x\mapsto x\cdot x$ 使 E 成为 $\mathbf{Z}$ 上的二次模 (见第四章定义 1, §1.1). 如果 (e_i) 是 E 的一组基而 $x=\sum x_ie_i$, 则二次型 $f(x)=x\cdot x$ 由公式

$$f(x)=\sum_{i,j}a_{ij}x_ix_j=\sum_i a_{ii}x_i^2+2\sum_{i<j}a_{ij}x_ix_j,\quad a_{ij}=e_i\cdot e_j$$

给出. 因此该式中非对角项的系数是偶数. f 的判别式 (即 $\det(a_{ij})$) 等于 ±1. 改变基 (e_i) 意味着矩阵 $A=(a_{ij})$ 代之以 ${}^tBAB$, 其中 $B\in\mathrm{GL}(n, \mathbf{Z})$. 从型 f 的观点, 这意味着将变量 (x_i) 作矩阵 B 的线性代换. 如此得到的型称为与型 f 等价.

(注意这是在整数环 $\mathbf{Z}$ 上的等价，它比前章中所研究的在 $\mathbf{Q}$ 上的等价要精细.)

1.2. S 上的运算

设 E, $E'\in S$. 以 $E\oplus E'$ 表示 E 与 E' 的直和，其双线性型是 E 与 E' 上双线性型的直和. 由定义可知(见 Bourbaki, 代数, 第九章 § 1, n°3):

$$(x+x')\cdot(y+y')=x\cdot y+x'\cdot y' \quad (x,\ y\in E,\ x',\ y'\in E').$$

从"二次型"的观点，这个运算对应于第四章中记成 $\hat{\oplus}$ 的正交直和.

我们还可以定义张量积 $E\otimes E'$ 与外积 $\wedge^m E$(见 Bourbaki, 代数，第九章 § 1, n°9). 但是我们不需要这些概念.

1.3. 不变量

1.3.1. 如果 $E\in S_n$, 整数 n 叫作 E 的秩，记成 $r(E)$.

1.3.2. 设 $E\in S$, 而令 $V=E\otimes\mathbf{R}$ 是系数从 $\mathbf{Z}$ 扩充为 $\mathbf{R}$ 而得到的 $\mathbf{R}$-向量空间. 则 V 的二次型可以定义符号量 (r, s) (第四章 § 2.4). 整数

$$\tau(E)=r-s$$

叫作 E 的符号差. 我们有

$$-r(E)\leqslant\tau(E)\leqslant r(E), \quad r(E)\equiv\tau(E) \pmod 2.$$

注意如果 $\tau(E)=\pm r(E)$, 即如果 $x\cdot x$ 不变符号，则 E 叫作是定的，否则 E 叫作是不定的.

1.3.3. E 对于一组基 (e_i) 的判别式不依赖于基的选择. 事实上，基 (e_i) 的改变是将判别式乘以 $\det({}^tXX)=\det(X)^2$, 其中 X 是 $\mathbf{Z}$ 上可逆矩阵. 而 X 的行列式等于 ±1, 从而其平方等于 1.

E 的判别式记成 $d(E)$，我们有 $d(E)=\pm 1$. 如果

$$V=E\otimes\mathbf{R}$$

的符号量为 (r,s)，则 $d(E)$ 的符号是 $(-1)^s$. 由于 $d(E)=\pm 1$，从而得到公式：

$$d(E)=(-1)^{\frac{r(E)-\tau(E)}{2}}.$$

1.3.4. 设 $E\in S$. 我们称 E 是偶类的(或叫作是第 II 类的)，是指与 E 所结合的二次型只取偶数值. 如果以 A 表示由 E 的一组基所定义的矩阵，这也可以说成：A 的对角元素均是偶数.

如果 E 不是偶类的，便称 E 是奇类的(或第 I 类的).

1.3.5. 设 $E\in S$ 而令 $\bar{E}=E/2E$ 为 E 的 mod 2 简化. 这是域 $\mathbf{F}_2=\mathbf{Z}/2\mathbf{Z}$ 上的 $r(E)$ 维向量空间. 转到商之后，型 $x\cdot y$ 在 $\bar{E}$ 上定义了型 $\bar{x}\cdot\bar{y}$，它是对称型并且判别式为 $\pm 1=1$. 它所结合的二次型 $\bar{x}\cdot\bar{x}$ 是加性的：

$$(\bar{x}+\bar{y})\cdot(\bar{x}+\bar{y})=\bar{x}\cdot\bar{x}+\bar{y}\cdot\bar{y}+2\bar{x}\cdot\bar{y}=\bar{x}\cdot\bar{x}+\bar{y}\cdot\bar{y}.$$

因此是 $\bar{E}$ 的对偶中的元素. 但是双线性型 $\bar{x}\cdot\bar{y}$ 非退化，它定义了 $\bar{E}$ 到其对偶之上的同构. 由此我们看出，存在一个正则元素 $\bar{u}\in\bar{E}$，使得

$$\bar{u}\cdot\bar{x}=\bar{x}\cdot\bar{x}\quad(\text{对一切 }\bar{x}\in\bar{E}).$$

将 $\bar{u}$ 提升到 E 之后，得到 mod $2E$ 唯一的元素 $u\in E$，使得

$$u\cdot x\equiv x\cdot x\ (\mathrm{mod}\ 2)\quad(\text{对一切 }x\in E).$$

考虑整数 $u\cdot u$. 如果 u 改成 $u+2x$，则 $u\cdot u$ 改成

$$(u+2x)\cdot(u+2x)=u\cdot u+4(u\cdot x+x\cdot x)\equiv u\cdot u\ (\mathrm{mod}\ 8).$$

于是 $u\cdot u$ 在 $\mathbf{Z}/8\mathbf{Z}$ 中的象是 E 的不变量. 我们将它记成 $\sigma(E)$. 如果 E 为第 II 类的，则型 $\bar{x}\cdot\bar{x}$ 为零 (换句话说，$x\cdot y$ 是交错型)，我们可以取 $u=0$，从而 $\sigma(E)=0$.

1.3.6. 设 p 为素数，令 $V_p = E\otimes\mathbf{Q}_p$ 是从 E 经过系数由 $\mathbf{Z}$ 扩充到 $\mathbf{Q}_p$ 之后而得到的 $\mathbf{Q}_p$- 向量空间. 那末在第四章 § 2.1 中定义的 V_p 的不变量 $\varepsilon(V_p)=\pm 1$ 也是 E 的不变量. 我们将它记为 $\varepsilon_p(E)$. 可以证明:

$$\varepsilon_p(E)=1 \quad (p\neq 2),$$

$$\varepsilon_2(E)=(-1)^j,$$

其中
$$j=\frac{1}{4}(d(E)+r(E)-\sigma(E)-1).$$

把 $E\otimes\mathbf{Z}_p$ 分解成一些秩 1 ($p\neq 2$ 时) 或秩为 1 和 2 (当 $p=2$ 时) 的 $\mathbf{Z}_p$-模的正交直和，就可以证出上面两个公式. 因为我们不使用这两个公式，把其证明细节留给读者 (还可见 J. Cassels, Comm. Math. Helv., 37, 1962, pp. 61～64).

1.3.7. 令 E_1, $E_2\in S$ 而 $E=E_1\oplus E_2$. 则 E 是第 II 类的$\Leftrightarrow E_1$ 和 E_2 都是第 II 类的. 而且有

$$r(E)=r(E_1)+r(E_2), \quad \tau(E)=\tau(E_1)+\tau(E_2).$$

$$\sigma(E)=\sigma(E_1)+\sigma(E_2), \quad d(E)=d(E_1)\cdot d(E_2).$$

1.4. 一些例子

1.4.1. 我们以 I_+ 和 I_- 分别表示 $\mathbf{Z}$-模 $\mathbf{Z}$ 连同双线性型 xy 和 $-xy$. 其对应的二次型分别为 $+x^2$ 和 $-x^2$.

如果 s 和 t 是两个正整数，我们以 $sI_+\oplus tI_-$ 表示 s 个 I_+ 与 t 个 I_- 的直和. 对应的二次型为 $\sum\limits_{i=1}^{s}x_i^2-\sum\limits_{j=1}^{t}y_j^2$. 这个模的不变量为

$$r=s+t, \quad \tau=s-t, \quad d=(-1)^t, \quad \sigma\equiv s-t \pmod 8).$$

除了平凡情形 $(s, t)=(0, 0)$ 之外，模 $sI_+\oplus tI_-$ 是第 I 类的.

1.4.2. 我们以 U 表示由矩阵 $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ 定义的 S_2 中元素，

其结合的二次型为 $2x_1x_2$. U 是第 II 类的，并且有

$$r(U)=2,\quad \tau(U)=0,\quad d(U)=-1,\quad \sigma(U)=0.$$

1.4.3. 设 k 为正整数，令 $n=4k$，令 V 为具有标准双线性型 $\sum x_iy_i$ 的向量空间 $\mathbf{Q}^n$，该双线性型对应于单位阵. 令 $E_0=\mathbf{Z}^n$ 是整坐标点所形成的 V 之子群，赋以由 V 所诱导的双线性型. 则 E_0 是 S_n 中元素，它同构于 nI_+. 设 E_1 为 E_0 之子模，由满足 $x\cdot x\equiv 0 \pmod 2$ (即 $\sum x_i\equiv 0 \pmod 2$) 的全部元素 x 所构成. 我们有 $(E_0:E_1)=2$. 令 E 是由 E_1 和

$$e=\left(\frac{1}{2},\ \cdots,\ \frac{1}{2}\right)$$

所生成的 V 之子模. 则 $2e\in E_1$ (由于 $n\equiv 0 \pmod 4$)，而 $e\notin E_1$，于是 $(E:E_1)=2$. 对于元素 $x=(x_i)\in V$，使 $x\in E$ 的充要条件为

$$2x_i\in\mathbf{Z},\quad x_i-x_j\in\mathbf{Z},\quad \sum_{i=1}^{n}x_i\in 2\mathbf{Z}.$$

于是有

$$x\cdot e=\frac{1}{2}\sum x_i\in\mathbf{Z}.$$

由于 $e\cdot e=k$，这表明型 $x\cdot y$ 在 E 上取整值. 此外，由于

$$(E_0:E_1)=(E:E_1),$$

从而 E 的判别式等于 E_0 的判别式，即为 $+1$. 因此二次模 E 是 $S_n=S_{4k}$ 中元素，我们将它记为 Γ_n. 如果 k 为偶数 (即 $n\equiv 0 \pmod 8$)，则 $e\cdot e=k$ 为偶数，这导致对于每个 $x\in E$，$x\cdot x$ 均为偶数. 因此当 $n\equiv 0 \pmod 8$ 时，Γ_n 是第 II 类的. 我们有

$$r(\Gamma_{8m})=8m,\quad \tau(\Gamma_{8m})=8m,$$
$$\sigma(\Gamma_{8m})=0,\quad d(\Gamma_{8m})=1.$$

Γ_8 的情形特别有趣. 共有 240 个元素[注] $x\in\Gamma_8$ 使 $x\cdot x=2$. 如果 (e_i) 表示 $\mathbf{Q}^8$ 的标准基，则这 240 个向量为

[注] 更一般地，我们在第七章 §6.5 中将要证明，如果 $N\geqslant 1$ 为整数，则 $\{x\in\Gamma_8 \mid x\cdot x=2N\}$ 中元数等于 N 之因子的立方和的 240 倍.

$$\pm e_i \pm e_k \quad (i \neq k)$$

和
$$\frac{1}{2}\sum_{i=1}^{8} \varepsilon_i e_i \quad \left(\varepsilon_i = \pm 1,\ \prod_{i=1}^{8} \varepsilon_i = 1\right).$$

[这些向量之间的内积均是整数．在李群理论中它们形成所谓“E_8型的根系”，见 Bourbaki，李群与李代数，第六章 § 4, n°10.]

可以把 Γ_8 的基取成

$$\frac{1}{2}(e_1+e_8)-\frac{1}{2}(e_2+\cdots+e_7), \quad e_1+e_2$$

和
$$e_i - e_{i-1} \quad (2 \leqslant i \leqslant 7),$$

对应的矩阵为

$$\begin{bmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{bmatrix}$$

对于 $m \geqslant 2$, $\{x \in \Gamma_{8m} \mid x \cdot x = 2\} = \{\pm e_i \pm e_k \mid i \neq k\}$．注意它们不生成 Γ_{8m}，这与 $m=1$ 的情形不同．特别地，$\Gamma_8 \oplus \Gamma_8$ 不同构于 Γ_{16}.

1.5. 群 $K(S)$

设 E, $E' \in S$．我们称 E 和 E' 是稳(stably)同构的，是指存在 $F \in S$，使 $E \oplus F \simeq E' \oplus F$，这是等价关系．我们以 $K_+(S)$ 表示 S 对这一关系之商．如果 $E \in S$，我们以 (E) 表

示 E 在 $K_+(S)$ 中的类. 运算 $\oplus$ 诱导出 $K_+(S)$ 上的运算 $+$, 这个运算满足交换律和结合律, 并且零元素是模 $0\in S$ 的类 0. 于是有

$$(E\oplus E')=(E)+(E').$$

此外, 如果 $x, y, z\in K_+(S)$, 使 $x+z=y+z$, 很容易证明 $x=y$. 这一点可使我们从半群 $K_+(S)$ 定义出群 $K(S)$ (恰好象从正整数集合 $\mathbf{Z}_+$ 定义出 $\mathbf{Z}$ 那样): 根据定义, $K(S)$ 中元素是元素对 (x, y), 其中 $x, y\in K_+(S)$, 两个元素对 (x, y) 和 (x', y') 等同 $\Leftrightarrow x+y'=y+x'$. $K(S)$ 中的运算定义为

$$(x, y)+(x', y')=(x+x', y+y').$$

这就把 $K(S)$ 作成交换群, 其零元素是 $(0, 0)$. 利用映射 $x\mapsto(x, 0)$, 我们把 $K_+(S)$ 等同于 $K(S)$ 的子集. $K(S)$ 中每个元素是 $K_+(S)$ 中两个元素之差, 从而可以写成形式 $(E)-(F)$, 其中 $E, F\in S$. 于是, 在 $K(S)$ 中

$$(E)-(F)=(E')-(F')$$

的充要条件是存在 $G\in S$, 使得 $E\oplus F'\oplus G\simeq E'\oplus F\oplus G$, 即相当于 $E\oplus F'$ 和 $E'\oplus F$ 是稳同构.

$K(S)$ 的万有性质. 设 A 是交换群而令 f: $S\to A$ 为函数, 使得 $E\simeq E_1\oplus E_2$ 时便有 $f(E)=f(E_1)+f(E_2)$. 这时我们称 f 是加性的. 如果 $X=(E)-(F)\in K(S)$, 我们令

$$f(X)=f(E)-f(F).$$

这不依赖于所选取的 X 的分解式. 显然如此定义的函数 f: $K(S)\to A$ 是一个同态. 反过来, 给了每个同态 f: $K(S)\to A$, 可以与 $S\to K(S)$ 合成为 S 上一个加性函数. 我们称 $K(S)$ 是 S 对于运算 $\oplus$ 的 Grothendieck 群, 以表达 $K(S)$ 的上述万有性质.

特别地, § 1.3 中的不变量 r, τ, d 和 σ 定义出同态:

$$r: K(S) \to \mathbf{Z}, \quad \tau: K(S) \to \mathbf{Z},$$
$$d: K(S) \to \{\pm 1\}, \quad \sigma: K(S) \to \mathbf{Z}/8\mathbf{Z}.$$

我们仍有 $\tau \equiv r \pmod 2$ 和 $d = (-1)^{\frac{r-\tau}{2}}$.

§2. 结果陈述

2.1. 群 $K(S)$ 的确定

定理 1 群 $K(S)$ 是以 (I_+) 和 (I_-) 为基的自由 Abel 群.

(证明将在 §3.4 中给出.)

换句话说, 每个 $f \in K(S)$ 均可唯一地写成

$$f = s \cdot (I_+) + t \cdot (I_-),$$

其中 s, $t \in \mathbf{Z}$. 于是有 $r(f) = s + t$, $\tau(f) = s - t$, 这表明 s 和 t 完全由 r 和 τ 确定. 由此即得

系 1 (r, τ) 定义了从 $K(S)$ 到 $\mathbf{Z} \times \mathbf{Z}$ 的子群

$$\{(a, b) \in \mathbf{Z} \times \mathbf{Z} \mid a \equiv b \pmod 2\}$$

之上的同构.

系 2 S 中两个元素 E 和 E' 稳同构的充要条件是它们有同样的秩和同样的符号差.

[注意由此不能推出 $E \simeq E'$. 例如

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

在 $K(S)$ 中与

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = I_+ \oplus I_-$$

定义出同样的元素, 但是 U 和 $I_+ \oplus I_-$ 有不同的奇偶类型.]

定理 2 对于每个 $E \in S$ 我们有 $\sigma(E) \equiv \tau(E) \pmod 8$.

证 事实上, τ 的 mod 8 简化以及 σ 均是从 $K(S)$ 到 $\mathbf{Z}/8\mathbf{Z}$ 中的同态, 它们在 $K(S)$ 的生成元 I_+ 和 I_- 上相等, 从

而它们一致.

系 1 如果 E 是第 II 类的, 则 $\tau(E)\equiv 0 \pmod 8$.

这是因为 $\sigma(E)=0$. (注意这导致 $r(E)\equiv 0 \pmod 2$ 和 $d(E)=(-1)^{r(E)/2}$.)

系 2 如果 E 是定的而且是第 II 类的, 则

$$r(E)\equiv 0 \pmod 8.$$

证 事实上, 如果 E 是定的, 我们有 $\tau(E)=\pm r(E)$.

注 1) 反过来, 我们在 § 1.4 中已看到, 对于每个

$$n\equiv 0 \pmod 8,$$

存在着 $E\in S_n$, 使 E 是正定的并且是第 II 类的.

2) 由乘积公式 $\prod \varepsilon_v(E)=1$ (见第四章 § 3.1) 和 § 1.3.6 中所给的 $\varepsilon_p(E)$ 值 (没有证明), 也可以推出同余式

$$\sigma(E)\equiv \tau(E) \pmod 8.$$

2.2. 结构定理(不定情形)

设 $E\in S$. 我们称 E 表示零, 如果存在 $x\in E$, $x\neq 0$, 使 $x\cdot x=0$. 这等价于说, 在第四章 § 1.6 的意义下, 其对应的二次型 $\mathbf{Q}(x)$ 在 $\mathbf{Q}$ 上表示 0. 基于齐次性质, 可以从一有理零点得到一个整零点.

定理 3 如果 $E\in S$ 是不定的, 则 E 表示零.

(证明将在 § 3.1 中给出.)

定理 4 如果 $E\in S$ 是不定的并且是第 I 类的, 则 E 同构于 $sI_+\oplus tI_-$, 其中 s, t 为 $\geqslant 1$ 的整数.

[于是对应的二次型在 $\mathbf{Z}$ 上等价于型 $\sum_{i=1}^{s} x_i^2-\sum_{j=1}^{t} y_j^2$.]

(证明将在 § 3.3 中给出.)

系 设 E 和 E' 为 S 中两个元素, 有同样的秩和符号量.

则或者 $E\oplus I_+\simeq E'\oplus I_+$, 或者 $E\oplus I_-\simeq E'\oplus I_-$.

证 如果 $E=0$, 这是显然的. 否则两个模 $E\oplus I_+$ 和 $E\oplus I_-$ 之中必有一个是不定的. 假设前一个是不定的. 由于 E 和 E' 有同样的符号量, 从而 $E'\oplus I_+$ 也是不定的. 利用定理 4 我们看出, $E\oplus I_+$ 和 $E'\oplus I_+$ 分别同构于 $sI_+\oplus tI_-$ 和 $s'I_+\oplus t'I_-$. 因为 E 和 E' 有同样的符号量, 我们有 $s=s'$ 和 $t=t'$, 从而即得结果.

定理 5 如果 $E\in S$ 是第 II 类的不定型, 并且 $\tau(E)\geqslant 0$, 则 E 同构于 $pU\oplus q\Gamma_8$, 其中 p 和 q 均为正整数.

[如果 $\tau(E)\leqslant 0$, 将此定理用于模 $-E$ 可得到一相应的结果, 这里 $-E$ 是从 E 将其二次型变号而得到的模.]

(证明将在 § 3.5 中给出.)

注意 $q=\dfrac{1}{8}\tau(E)$, $p=\dfrac{1}{2}(r(E)-\tau(E))$. 这表明不计同构 E 可由它的秩和符号差完全确定. 因为这对第 I 类是同样正确的(见定理 4), 我们得到

定理 6 如果 E, $E'\in S$ 是不定的, 并且有同样的秩、符号差和奇偶类, 则它们同构.

2.3. 定的情形

这时没有结构定理, 而只有"有限性"定理: 对于每个整数 n, S_n 只包含有限多个正定等价类. 这可从二次型的"化简理论"得到. 只是对小 n 值明显确定出了这些等价类 (对于 $n\leqslant 16$, 见 M. Kneser, Archiv der Math., 8, 1957, pp. 241～250). 我们可以从 Minkowski-Siegel 公式得出这些结果 (Kneser 使用了一个不同的方法). 现在叙述这个公式(为简单起见, 我只限于讨论第 II 类, 对于第 I 类有类似结果):

令 $n=8k$. 以 C_n 表示第 II 类正定型 $E\in S_n$ 之同构类集合. 如果 $E\in C_n$, 以 G_E 表示 E 的自同构群. 因为它是正交群的离散子群, 而正交群本身是紧致群, 从而 G_E 为有限群. 以 g_E 表示群 G_E 的阶数. 令

$$M_n=\sum_{E\in C_n}\frac{1}{g_E}.$$

这是 C_n 在 Eisenstein 意义下的"质量", 即 C_n 中元素 E 的个数, 但是每个元素 E 赋以权 $1/g_E$. Minkowski-Siegel 公式[注]给出 M_n 的值:

$$(*)\qquad M_n=\frac{B_{2k}}{8k}\prod_{j=1}^{4k-1}\frac{B_j}{4j},$$

其中 $n=8k$, 而 B_j 是 Bernoulli 数 $\left(B_1=\frac{1}{6},\ B_2=\frac{1}{30},\ \cdots,\right.$ 见第七章 § 4.1$\left.\right)$.

(下面是 M_n 的一些近似值:

$M_8=10^{-9}\times 1.4352\cdots$; $M_{16}=10^{-18}\times 2.4885\cdots$;

$M_{24}=10^{-15}\times 7.9369\cdots$; $M_{32}=10^{7}\times 4.0309\cdots$;

$M_{40}=10^{51}\times 4.3930\cdots$.)

这个公式给出一个方法来证明何时 C_n 的一个子集 C' 等于 C_n, 这只需对于 $E\in C'$ 检查 $1/g_E$ 之和是否等于 M_n (因为如果 $C'\neq C_n$, 则该和式 $<M_n$).

【例】

i) $n=8$, 即 $k=1$. 可以证明(例如见 Bourbaki, 李群与李代数, 第六章 § 4, n°10), Γ_8 的自同构群的阶数是 $2^{14}3^5 5^2 7$. 而公式 (*) 给出 $M_8=2^{-14}3^{-5}5^{-2}7^{-1}$. 比较一下即知 C_8 只有一个元素 Γ_8, 这是 Mordell 的结果.

[注] 这个公式的证明可见 C. L. Siegel, Gesamm. Abh., I, n°20 和 III, n° 79.

ii) $n=16$. 我们已知 C_{16} 中的两个元素：Γ_{16} 和 $\Gamma_8\oplus\Gamma_8$. 可以证明其阶数 g_E 分别为 $2^{15}(16!)$ 和 $2^{29}3^{10}5^47^2$. 而

$$M_{16}=691\cdot2^{-30}3^{-10}5^{-4}7^{-2}11^{-1}13^{-1}.$$

容易检查

$$691/2^{30}3^{10}5^47^211\cdot13=1/2^{15}(16!)+1/2^{29}3^{10}5^47^2.$$

因此我们有 $C_{16}=\{\Gamma_{16},\ \Gamma_8\oplus\Gamma_8\}$, 这是 Witt 的结果.

iii) $n=24$. 1957 年 H. Niemeier 确定出 C_{24}. 该集合共有 24 个元素. 其中有一个元素特别值得注意(由 Leech 研究 $\mathbf{R}^{24}$ 之球覆盖问题时所发现), 它也是 C_{24} 中唯一的元素不包括满足 $x\cdot x=2$ 的向量 x. 它的自同构群 G 的阶数为

$$2^{22}3^95^47^211\cdot13\cdot23=8,315,553,613,086,720,000.$$

商群 $G/\{\pm1\}$ 是由 Conway[注] 发现的新的单群.

iv) $n=32$. 由于 $M_{32}>4\cdot10^7$, 并且对于每个 E 均有 $g_E\geqslant2$, 因此 C_{32} 有多于 8 千万个元素. 目前还不能把它们分类.

§3. 证　　明

3.1. 定理 3 的证明

令 $E\in S_n$, 而 $V=E\otimes\mathbf{Q}$ 是对应的 $\mathbf{Q}$-向量空间. 假设 E 是不定的. 我们必需证明 E(或者 V)表示零. 这要改虑一系列情形:

i) $n=2$. 这时 V 的符号量是(1, 1), 从而 $d(E)=-1$. 由于 $-d(E)$ 为 $\mathbf{Q}$ 中平方元素, 显然 V 表示 0.

ii) $n=3$. 设 $f(X_1,\ X_2,\ X_3)=\sum a_{ij}X_iX_j$ 是关于 E 之一组基所对应的二次型. 我们有 $a_{ij}\in\mathbf{Z}$ 而 $\det(a_{ij})=\pm1$. 如

[注] 见 J. H. Conway, Proc. Nat. Acad. Sci. USA, 61, 1968, pp. 398～400, 和 Invent. Math., 7, 1969, pp. 137～142.

果 $p\neq 2$ 是素数，由 f 之 mod 2 简化所得到的型有非平凡零点（第一章 § 2.2），这个零点可以提升成 p-adic 零点（第二章 § 2.2，定理 1 的系 2）．于是对于每个 $\mathbf{Q}_p(p\neq 2)$ 和 $\mathbf{R}$，f 均表示 0．由第四章 § 3.2，定理 8 的系 3，可知 f 在 $\mathbf{Q}$ 中表示 0．

iii) $n=4$．同上可证对于每个 $\mathbf{Q}_p(p\neq 2)$ 和 $\mathbf{R}$，二次型 f 均表示 0．如果 f 的判别式 $d(E)=1$，这就可以推出 f 在 $\mathbf{Q}$ 中表示 0（第四章 § 3.2 定理 8 的系 3）．否则我们有 $d(E)=-1$，而 $d(E)$ 不是 $\mathbf{Q}_2$ 中平方元素．由第四章 § 2.2 定理 6，这导致 f 在 $\mathbf{Q}_2$ 中表示 0．于是由 Hasse-Minkowski 定理（第四章 § 3.2 定理 8）可知 f 在 $\mathbf{Q}$ 中表示 0．

iv) $n\geqslant 5$．用 Meyer 定理（第四章 § 3.2 定理 8 的系 2）．

3.2．一些引理

设 $E\in S$，令 F 为 E 的子模．F' 是 E 中与整个 F 正交的元素所构成的子集．

引理 1　F 赋以 E 所诱导的型 $x\cdot y$ 之后属于 S 的充要条件是 E 为 F 与 F' 的直和．

证　如果 $E=F\oplus F'$，则 $d(E)=d(F)\cdot d(F')$，由此即知 $d(F')=\pm 1$．反之，如果 $d(F)=+1$，显然 $F\cap F'=0$．此外，如果 $x\in E$，则线性变换 $y\mapsto x\cdot y\,(y\in F)$ 可以由一个元素 $x_0\in F$ 所决定．于是我们有 $x=x_0+x_1$，其中 $x_0\in F$，$x_1\in F'$，从而 $E=F\oplus F'$．

引理 2　设 $x\in E$ 满足 $x\cdot x=\pm 1$，而 X 是 x 在 E 中的正交补．如果 $D=\mathbf{Z}x$，则 $E=D\oplus X$．

证　将引理 1 用于 $F=D$ 即可．（比如若 $x\cdot x=1$，则有 $D\simeq I_+$，于是 $E\simeq I_+\oplus X$．）

$x\in X$ 称为不可除元素，如果它不在每个子群 $nE\,(n\geqslant 2)$

中，即如果它不能被某个$\geqslant 2$的整数所除尽. E中每个非零元素均可唯一地写成形式mx, 其中$m\geqslant 1$, 而x为不可除元素.

引理 3 如果x为E中不可除元素，则存在$y\in E$, 使

$$x\cdot y=1.$$

证 令f_x是由x所决定的线性映射$y\mapsto x\cdot y$. 这是$E\to \mathbf{Z}$的同态. 由于x的不可除性和$x\cdot y$定义了E到其对偶$\mathrm{Hom}(E, \mathbf{Z})$之上的同构，可知$f_x$也是不可除的. 由此即知$f_x$是映上(不然，它可以由一个$\geqslant 2$的整数所除尽)，因此存在$y\in E$, 使$x\cdot y=1$.

3.3. 结构定理(奇不定情形[注])

引理 4 设$E\in S_n$. 而E是第I类的和不定的，则存在$F\in S_{n-2}$, 使$E\sim I_+\oplus I_-\oplus F$.

证 根据定理 3, 存在$x\in E$, $x\neq 0$, 使得$x\cdot x=0$. 必要时将x除以一个整数，我们可以假定x是不可除的. 根据上面的引理 3, 可知这时存在$y\in E$, 使$x\cdot y=1$. 我们可以选取y使$y\cdot y$为奇数. 事实上，假如$y\cdot y$是偶数，因为E是第I类的，从而存在$t\in E$, 使$t\cdot t$为奇数. 令$y'=t+ky$, 并且取k使$x\cdot y'=1$, 即取$k=1-x\cdot t$. 我们有$y'\cdot y'\equiv t\cdot t \pmod 2$, 而$y'\cdot y'$为奇数. 于是我们可以假定$y\cdot y=2m+1$. 这时令

$$e_1=y-mx, \qquad e_2=y-(m+1)x.$$

立刻得到$e_1\cdot e_1=1$, $e_1\cdot e_2=0$, $e_2\cdot e_2=-1$. 由(e_1, e_2)生成的E的子模G同构于$I_+\oplus I_-$; 按照引理 1, 便有$E\simeq I_+\oplus I_-\oplus F$, 其中$F\in S_{n-2}$.

定理 4 的证明. 我们对于n用数学归纳法. 令$E\in S_n$,

[注] 本节中所述方法以及引进群$K(S)$的思想，都是 Milnor 告诉我的.

并且设 E 是不定的第 I 类的. 根据引理 4,

$$E\simeq I_+\oplus I_-\oplus F.$$

如果 $n=2$, 则 $F=0$, 从而定理证毕. 如果 $n>2$, 则 $F\neq 0$, 并且模 $I_+\oplus F$ 和 $I_-\oplus F$ 必有一个是不定的, 例如设第一个是不定的. 因为 I_+ 是第 I 类的, $I_+\oplus F$ 亦如此. 利用归纳假设可证得 $I_+\oplus F$ 有形式 $aI_+\oplus bI_-$, 这就证明了

$$E\simeq aI_+\oplus(b+1)I_-.$$

3.4. 群 $K(S)$ 的确定

设 $E\in S$, $E\neq 0$. 则 $E\oplus I_+$ 或 $E\oplus I_-$ 中有一个是不定的第 I 类的. 利用定理 4 我们看到 E 在 $K(S)$ 中的象是 (I_+) 与 (I_-) 的线性组合. 这就表明 (I_+) 和 (I_-) 生成 $K(S)$. 由于它们在同态

$$(r,\ \tau):\ K(S)\to\mathbf{Z}\times\mathbf{Z}$$

之下的象是线性无关的, 从而 (I_+) 和 (I_-) 形成 $K(S)$ 的一组基.

3.5. 结构定理(偶不定情形)

引理 5 设 $E\in S$, E 是不定的和第 II 类的, 则存在 $F\in S$, 使 $E\simeq U\oplus F$.

证 与引理 4 的证明过程相仿. 先取 $0\neq x\in E$, x 不可除, 使 $x\cdot x=0$. 再取 $y\in E$, 使 $x\cdot y=1$. 如果 $y\cdot y=2m$, 我们用 $y-mx$ 代替 y, 对于这个新的 y 有 $y\cdot y=0$. 于是由 $(x,\ y)$ 生成的 E 之子模 G 同构于 U. 由引理 1 即知 $E\simeq U\oplus F$, 其中 $F\in S$.

引理 6 设 F_1, $F_2\in S$. F_1 和 F_2 均是第 II 类的, 并且 $I_+\oplus I_-\oplus F_1\simeq I_+\oplus I_-\oplus F_2$, 则 $U\oplus F_1\simeq U\oplus F_2$.

证 为简化符号我们令

$$W=I_+\oplus I_-,\quad E_i=W\oplus F_i,\quad V_i=E_i\otimes\mathbf{Q}.$$

在 E_i 中，令 E_i^0 表示 E_i 中满足 $x\cdot x\equiv 0 \pmod 2$ 的元素 x 所构成的子群. 则 $(E_i:E_i^0)=2$. 不难看出 $E_i^0=W^0\oplus F_i$, 其中

$$W^0=\{x=(x_1,\ x_2)\in W \mid x_1\equiv x_2 \pmod 2\}.$$

令 E_i^+ 为 E_i^0 在 V_i 中的"对偶"，即

$$E_i^+=\{y\in V_i \mid x\cdot y\in\mathbf{Z},\ 对一切\ x\in E_i^0\}.$$

显然 $E_i^+=W^+\oplus F_i$, 其中

$$W^+=\{(x_1,\ x_2)\mid 2x_1,\ 2x_2,\ x-x_2\in\mathbf{Z}\}.$$

我们有 $E_i^0\subset E_i\subset E_i^+$, 并且商 E_i^+/E_i^0 同构于 W^+/W_0. 这是 $(2,\ 2)$ 型群. 因此在 E_1^0 和 E_i^+ 之间严格地有三个子群，它们对应于 $(2,\ 2)$ 型群中的 3 个 2 阶子群. E_i 本身是其中的一个. 我们把另外两个记成 E_i' 和 E_i''. 于是又有

$$E_i'=W'\oplus F_i,\quad E_i''=W''\oplus F_i.$$

其中 W' 和 W'' 以明显的方式定义. 可以验证 W' 和 W'' 均同构于 $U\left(例如取\ W'\ 的一组基为向量\ a=\left(\frac{1}{2},\ \frac{1}{2}\right)和\ b=(1,\ -1)\right.$. 我们有 $a\cdot a=b\cdot b=0,\ a\cdot b=1$. 对于 W'' 则取 $\left.\left(\frac{1}{2},\ -\frac{1}{2}\right)和(1,\ 1)\right)$. 然后令 $f: W\oplus F_1\to W\oplus F_2$ 为同构，它可扩充成 V_1 到 V_2 上的同构，并且将 E_1 映到 E_2 之上，从而也把 E_1^0 和 E_1^+ 分别映到 E_2^0 和 E_2^+ 之上，于是它也把 $(E_1',\ E_1'')$ 映到 $(E_2',\ E_2'')$ 或者 $(E_2'',\ E_2')$ 之上. 由于 E_i' 和 E_i'' 均同构于 $U\oplus F_i$, 从而 $U\oplus F_1\simeq U\oplus F_2$.

定理 5 的证明. 我们先证，如果 $E_1,\ E_2\in S$ 是第 II 类的不定的，并且有同样的秩和符号差，则它们同构.

由引理 5 我们有 $E_1=U\oplus F_1,\ E_2=U\oplus F_2$. 显然 F_1 和

F_2 是第 II 类的，而且有同样的秩和符号差．模

$$I_+ \oplus I_- \oplus F_1 \quad \text{和} \quad I_+ \oplus I_- \oplus F_2$$

是第 I 类的，不定的，而且有相同的秩和符号差．根据定理 4 它们同构．利用引理 6 我们看出 E_1 和 E_2 同构，这就证明了我们的论断．

现在定理 5 就显然了：如果 E 是不定的和第 II 类的，并且 $\tau(E) \geqslant 0$，我们可以由公式

$$q = \frac{1}{8}\tau(E), \quad p = \frac{1}{2}(r(E) - \tau(E))$$

确定出整数 p 和 q．将上述结果用于 E 和 $pU \oplus q\Gamma_8$，即知这两个模是同构的．

第二部分

解析方法

第六章　算术级数中的素数定理

本章的目的是要证明如下的定理，这个定理是由 Legendre 猜想(和使用)而由 Dirichlet 证明的.

定理　设 a 和 m 是互素的两个自然数. 则存在无限多个素数 $p\equiv a \pmod m$.

我们采取的方法是利用 L 函数的一些性质(这正是 Dirichlet 本人的方法).

§1.　有限 Abel 群的特征

1.1. 对偶性

设 G 为有限 Abel 群,其运算写成乘法.

定义 1　G 的特征是 G 到复数乘法群 $\mathbf{C}^*$ 中的同态.

G 的全部特征形成群 $\mathrm{Hom}(G, \mathbf{C}^*)$, 我们写成 $\hat{G}$, 叫作 G 的对偶.

【例】　设 G 是生成元为 s 的 n 阶循环群. 如果 $\chi: G\to\mathbf{C}^*$ 是 G 的特征,则元素 $w=\chi(s)$ 满足关系 $w^n=1$, 即 w 是 n 次单位根. 反之,每个 n 次单位根 w 利用 $s^a\mapsto w^a$ 均可定义 G 的一个特征. 于是我们看到, 映射 $\chi\mapsto\chi(s)$ 是 $\hat{G}$ 到 n 次单位根群 μ_n 之上的同构. 特别地, $\hat{G}$ 是 n 阶循环群.

命题 1　设 H 为 G 的子群, 则 H 的每个特征均可扩充成 G 的特征.

证　我们对于 $(G:H)$ 归纳. 如果 $(G:H)=1$, 则 $G=H$, 从而没有什么可证的. 否则我们令 $x\in G$, $x\notin H$, 命 n 为使

$x^n \in H$ 成立的 >1 的最小整数. 设 χ 是 H 的特征，令

$$t=\chi(x^n).$$

由于 $\mathbf{C}^*$ 是可除群，我们可以取一元素 $w\in\mathbf{C}^*$，使 $w^n=t$. 令 H' 是由 H 和 x 生成的 G 之子群. H' 中每个元素 h' 均可以写成 $h'=hx^a$，其中 $h\in H$ 而 $a\in\mathbf{Z}$. 令

$$\chi'(h')=\chi(h)w^a,$$

易知这个数与 h' 的分解 hx^a 无关，而且 $\chi':H'\to\mathbf{C}^*$ 是 H' 的特征，并且为 χ 的扩充. 由于 $(G:H')<(G:H)$，利用归纳假设便知 χ' 可扩充为整个 G 的特征.

注 限制运算定义出一个同态

$$\rho:\ \hat{G}\to\hat{H},$$

而命题 1 表明 ρ 是映上. 此外，ρ 的核是在 H 上平凡的 G 的那些特征所组成的集合，从而它同构于 G/H 之对偶群 $(\widehat{G/H})$. 于是有正合列

$$\{1\}\to(\widehat{G/H})\to\hat{G}\to\hat{H}\to\{1\}.$$

命题 2 群 $\hat{G}$ 是有限 Abel 群，其阶数与 G 相同.

证 对于 G 的阶数 n 进行归纳. $n=1$ 的情形是显然的. 如果 $n\geqslant 2$，取 G 的一个非平凡循环子群 H. 根据上面的注记，$\hat{G}$ 的阶数为 $\hat{H}$ 的阶数与 $(\widehat{G/H})$ 的阶数之乘积. 但是由于 H 是循环群，而 G/H 的阶数严格小于 n，从而它们的阶数均与其对偶的阶数相同. 因此 $\hat{G}$ 的阶数等于 H 的阶数与 G/H 的阶数之乘积，即等于 G 的阶数.

注 利用 G 分解成循环群的乘积，可以证明更精密的结果：$\hat{G}$（一般非自然地）同构于 G.

如果 $x\in G$，则函数 $\chi\mapsto\chi(x)$ 是 $\hat{G}$ 的特征. 我们便得到一个同态 $\varepsilon:\ G\to\hat{\hat{G}}$.

命题 3 同态 ε 是 G 到 $\hat{\hat{G}}$ 上的同构.

证 由于 G 和 $\hat{\hat{G}}$ 的阶数相同，只需证明 ε 是单射，即如果 $1\neq x\in G$，存在 G 的一个特征 χ 使得 $\chi(x)\neq 1$. 现在令 H 是 G 的由 x 生成的循环子群. 显然(见上面例子) 存在 H 的一个特征 χ 使得 $\chi(x)\neq 1$. 而命题 1 表明 χ 可以扩充成 G 的特征，由此即得所需结果.

1.2. 正交关系

命题 4 设 $n=\mathrm{Card}(G)$，$\chi\in\hat{G}$，则

$$\sum_{x\in G}\chi(x)=\begin{cases} n, & \text{如果 } \chi=1, \\ 0, & \text{如果 } \chi\neq 1. \end{cases}$$

证 第一个公式显然. 为证第二个公式，取 $y\in G$，使

$$\chi(y)\neq 1.$$

则有 $$\chi(y)\sum_{x\in G}\chi(x)=\sum_{x\in G}\chi(xy)=\sum_{x\in G}\chi(x).$$

于是 $$(\chi(y)-1)\sum_{x\in G}\chi(x)=0.$$

因为 $\chi(y)\neq 1$，由此导致 $\sum\limits_{x\in G}\chi(x)=0$.

系 设 $x\in G$，则

$$\sum_{\chi\in\hat{G}}\chi(x)=\begin{cases} n, & \text{如果 } x=1, \\ 0, & \text{如果 } x\neq 1. \end{cases}$$

证 将命题 4 用于对偶群 $\hat{G}$ 即可.

注 上面结果是(不必 Abel 的)有限群特征理论中的“正交关系”之特殊情形.

1.3. 模特征

设 $m\geqslant 1$ 为整数. 以 $G(m)$ 表示环 $\mathbf{Z}/m\mathbf{Z}$ 的可逆元所构成的乘法群 $(\mathbf{Z}/m\mathbf{Z})^*$. 这是 $\phi(m)$ 阶 Abel 群，其中 $\phi(m)$ 是

m的 Euler ϕ 函数，见第一章 § 1.2.. $G(m)$之对偶中的元素 χ 叫作是 mod m 特征. 可以把它看成定义在与 m 互素的整数集合上而取值于 $\mathbf{C}^*$ 的函数，并且 $\chi(ab)=\chi(a)\chi(b)$. 为方便起见，可将它扩充成整个 $\mathbf{Z}$ 上的函数，即当 a 不与 m 互素时，我们令 $\chi(a)=0$.

一些例子

1) $m=4$. 群 $G(4)$有两个元素，从而只有唯一的一个非平凡特征，即 $x\mapsto(-1)^{\varepsilon(x)}$，见第一章 § 3.2.

2) $m=8$. 群 $G(8)$ 有 4 个元素. 它有三个非平凡特征，即

$$x\mapsto(-1)^{\varepsilon(x)},\ (-1)^{\omega(x)},\ (-1)^{\varepsilon(x)+\omega(x)}.$$

见第一章 § 3.2.

3) $m=p$, $p\neq 2$ 为素数. 群 $G(p)$是 $p-1$ 阶循环群，从而有唯一的一个 2 阶特征，即 Legendre 特征 $x\mapsto\left(\frac{x}{p}\right)$.

4) $m=7$. 群 $G(7)$ 为 6 阶循环群，因此有两个彼此共轭的 3 阶特征. 其中一个为

$$\chi(x)=\begin{cases}1, & \text{如果 } x\equiv\pm1 \pmod 7,\\ e^{\frac{2\pi i}{3}}, & \text{如果 } x\equiv\pm2 \pmod 7,\\ e^{\frac{4\pi i}{3}}, & \text{如果 } x\equiv\pm3 \pmod 7.\end{cases}$$

2 阶特征与 Legendre 特征有紧密的联系. 更确切地说:

命题5 设 a 是无平方因子的非零整数（见第四章 § 3.2），$m=4|a|$. 则存在唯一的一个 mod m 特证 χ_a，使对每个除不尽 m 的素数 p 均有 $\chi_a(p)=\left(\frac{a}{p}\right)$. 此外还有 $\chi_a^2=1$，并且 $a\neq1$ 时 $\chi_a\neq1$.

证 χ_a 的唯一性显然，因为每个与 m 互素的整数均是除

不尽m的一些素数之积. 同理可证 $\chi_a^2=1$.

为证 χ_a 的存在性，先设 $a=l_1\cdots l_k$，其中 l_i 为彼此不同的奇素数. 然后我们取特征

$$\chi_a(x)=(-1)^{\varepsilon(x)\varepsilon(a)}\left(\frac{x}{l_1}\right)\cdots\left(\frac{x}{l_k}\right).$$

如果 p 为奇素数且不等于任何一个 l_i，由二次互反律有

$$\chi_a(p)=\left(\frac{l_1}{p}\right)\cdots\left(\frac{l_k}{p}\right)=\left(\frac{a}{p}\right),$$

从而这个 χ_a 即有所需性质.

如果 a 有形式 $-b$, $2b$ 或者 $-2b$，其中 $b=l_1\cdots l_k$ 如前所示. 我们分别取 χ_a 为 χ_b 和

$$(-1)^{\varepsilon(x)},\quad (-1)^{\omega(x)}\quad 或者\quad (-1)^{\varepsilon(x)+\omega(x)}$$

之积. χ_a 的这个明显结构也同时表明当 $a\neq 1$ 时，$\chi_a\neq 1$.

注 可以证明，如果 $x>0$ 为与m互素的整数，则

$$\chi_a(x)=\prod_{l\mid m}(a,\ x)_l=\prod_{(l,m)=1}(a,\ x)_l,$$

其中 $(a,\ x)_l$ 是 a 和 x 在域 $\mathbf{Q}_l$ 中的 Hilbert 符号. 这个公式可以用来作为 χ_a 的定义.

§2. Dirichlet 级数

2.1. 一些引理

引理 1 设 U 为 $\mathbf{C}$ 的开子集，f_n 是 U 上全纯函数序列，它们在每个紧集上均一致收敛于函数 f，则 f 在 U 中全纯且 f_n 的导函数 f_n' 在每个紧子集上也一致收敛于 f 的导函数 f'.

我们回忆一下它的证明概要.

设 D 是 U 中的闭圆盘，令 C 是它按通常方式取向的有向边界. 由 Cauchy 公式，对 D 的每个内点 z_0 我们有

$$f_n(z_0)=\frac{1}{2\pi i}\int_C\frac{f_n(z)}{z-z_0}dz.$$

通过极限过程便得到

$$f(z_0)=\frac{1}{2\pi i}\int_C\frac{f(z)}{z-z_0}dz.$$

这证明 f 在 D 的内部全纯，从而证明了引理的第一部分. 利用公式

$$f'(z_0)=\frac{1}{2\pi i}\int_C\frac{f(z)}{(z-z_0)^2}dz,$$

我们同法可证第二部分.

引理 2(Abel 引理) 设(a_n)和(b_n)是两个数列. 令

$$A_{m,p}=\sum_{n=m}^{p}a_n,\quad S_{m,m'}=\sum_{n=m}^{m'}a_nb_n,$$

则
$$S_{m,m'}=\sum_{n=m}^{m'-1}A_{m,n}(b_n-b_{n+1})+A_{m,m'}b_{m'}.$$

证 易 a_n 为 $A_{m,n}-A_{m,n-1}$ 然后重新组织各项即可.

引理 3 设 α, β 是两个实数, $0<\alpha<\beta$, 令 $z=x+iy$, 其中 x, $y\in\mathbf{R}$, $x>0$. 则

$$|e^{-\alpha z}-e^{-\beta z}|\leqslant\left|\frac{z}{x}\right|(e^{-\alpha x}-e^{-\beta x}).$$

证 记

$$e^{-\alpha z}-e^{-\beta z}=-z\int_\alpha^\beta e^{-tz}dt,$$

然后取绝对值即有

$$|e^{-\alpha z}-e^{-\beta z}|\leqslant|z|\int_\alpha^\beta e^{-tx}dt=\frac{|z|}{x}(e^{-\alpha x}-e^{-\beta x}).$$

2.2. Dirichlet 级数

设(λ_n)是趋于 $+\infty$ 的递增实数列. 为简单起见，我们假定 λ_n 均>0 (这不是本质的限制，因为我们在后面讨论中，总

可以去掉数列的有限多项而化成上述情形)。

指数为(λ_n)的 Dirichlet 级数是指具有下面形式的级数:

$$\sum a_n e^{-\lambda_n z} \quad (a_n \in \mathbf{C},\ z \in \mathbf{C}).$$

【例】 (a) $\lambda_n = \log n$(通常的 Dirichlet 级数)。这样一个级数可写成$\sum \frac{a_n}{n^z}$, 见 § 2.4.

(b) $\lambda_n = n$. 取$t = e^{-z}$, 则级数变成对于t的幂级数。

注 Dirichlet 级数是测度μ的 Laplace 变换

$$\int_0^\infty e^{-zt} \mu(t)$$

的特殊情形, 在我们这里μ为离散测度(详见 D. Widder, The Laplace Transform, 1946).

命题 6 如果级数$f(z) = \sum a_n e^{-\lambda_n z}$对于$z = z_0$收敛, 则它在形如$\mathrm{Re}(z - z_0) \geqslant 0$, $|\mathrm{Arg}(z - z_0)| \leqslant \alpha\ (\alpha < \pi/2)$的每个区域中均一致收敛.

(此处及以后我们用$\mathrm{Re}(z)$表示复数z的实数部分.)

证 对z作一变量代换, 可设$z_0 = 0$. 于是假设条件变成级数$\sum a_n$收敛. 我们必须证明级数在形如

$$\mathrm{Re}(z) \geqslant 0, \quad |z|/\mathrm{Re}(z) \leqslant k$$

的区域中一致收敛. 令$\varepsilon > 0$. 因为级数$\sum a_n$收敛, 从而存在N, 使当m, $m' \geqslant N$时, 我们有$|A_{m,m'}| \leqslant \varepsilon$(记号见引理 2). 对于$b_n = e^{-\lambda_n z}$利用引理 2, 我们得到

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n} (e^{-\lambda_n z} - e^{-\lambda_{n+1} z}) + A_{m,m'} e^{-\lambda_{m'} z}.$$

令$z = x + iy$并利用引理 3, 我们发现

$$|S_{m,m'}| \leqslant \varepsilon \left(1 + \frac{|z|}{x} \sum_{n=m}^{m'-1} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x})\right),$$

即 $$|S_{m,m'}|\leqslant\varepsilon(1+k(e^{-\lambda_m x}-e^{-\lambda_{m'}x})),$$
于是 $|S_{m,m'}|\leqslant\varepsilon(1+k)$. 而一致收敛性是显然的.

系 1 如果 f 对于 $z=z_0$ 收敛，则它对于 $\mathrm{Re}(z)>\mathrm{Re}(z_0)$ 收敛,而这样定义的函数是全纯的.

证 这可由命题 6 和引理 1 推出.

系 2 级数 f 的收敛区域包含一个最大的开半平面（称为该级数的收敛半平面).

(为了语言上的方便，我们把 ϕ 和 $\mathbf{C}$ 也看作是开半平面.)

如果收敛半平面由 $\mathrm{Re}(z)>\rho$ 给出,我们称 ρ 为该级数的收敛横坐标.

(情形 ϕ 和 $\mathbf{C}$ 分别对应于 $\rho=+\infty$ 和 $\rho=-\infty$.)

级数 $\sum|a_n|e^{-\lambda_n z}$ 的收敛半平面（由于明显的理由）称作 f 的绝对收敛半平面. 它的收敛横坐标记成 ρ^+. 当 $\lambda_n=n$ 时（幂级数)，熟知 $\rho=\rho^+$. 而对于一般情形这是不对的. 例如我们以后将知道,最简单的 L-级数

$$L(z)=1-\frac{1}{3^z}+\frac{1}{5^z}-\frac{1}{7^z}+\cdots,$$

其 $\rho=0$, 而 $\rho^+=1$.

系 3 在区域

$$\mathrm{Re}(z-z_0)\geqslant 0,\qquad |\mathrm{Arg}(z-z_0)|\leqslant\alpha\quad(\alpha<\pi/2)$$

中 $z\to z_0$ 时，$f(z)\to f(z_0)$.

证 这由一致收敛性和 $e^{-\lambda_n z}\to e^{-\lambda_n z_0}$ 这一事实推出.

系 4 $f(z)=0\Leftrightarrow a_n$ 均为 0.

证 先证 $a_0=0$. 将 f 乘以 $e^{\lambda_0 z}$ 然后令 $z\to+\infty$（例如取 z 为实数). 由一致收敛性可知 $e^{\lambda_0 z}f\to a_0$, 从而 $a_0=0$. 对 a_1 等等可以类似地去作.

2.3. 正系数的 Dirichlet 级数

命题 7 设 $f=\sum a_n e^{-\lambda_n z}$ 是 Dirichlet 级数，其系数 a_n 为非负实数. 假定 f 对于 $\mathrm{Re}(z)>\rho(\rho\in\mathbf{R})$ 收敛，并且函数 f 可解析开拓成一个在点 $z=\rho$ 某邻域中全纯的函数，则存在 $\varepsilon>0$，使 f 在 $\mathrm{Re}(z)>\rho-\varepsilon$ 中收敛.

(换句话说，f 之收敛区域由 f 在实轴上的奇异点所界.)

证 将 z 代之以 $z-\rho$，我们可设 $\rho=0$. 因为 f 在 $\mathrm{Re}(z)>0$ 和在 0 的某邻域中全纯，从而它在圆盘

$$|z-1|\leqslant 1+\varepsilon \quad (\varepsilon>0)$$

中全纯. 特别地，它的 Taylor 级数在这个圆盘中收敛. 由引理 1，f 的 p 阶导函数为

$$f^{(p)}(z)=\sum_n a_n(-\lambda_n)^p e^{-\lambda_n z} \quad (\text{对于 } \mathrm{Re}(z)>0),$$

于是

$$f^{(p)}(1)=(-1)^p\sum_n \lambda_n^p a_n e^{-\lambda_n}.$$

在问题中的 Taylor 级数可以写成

$$f(z)=\sum_{p=0}^{\infty}\frac{1}{p!}(z-1)^p f^{(p)}(1), \quad |z-1|\leqslant 1+\varepsilon.$$

特别对于 $z=-\varepsilon$，我们有

$$f(-\varepsilon)=\sum_{p=0}^{\infty}\frac{1}{p!}(1+\varepsilon)^p(-1)^p f^{(p)}(1),$$

此级数收敛.

但是 $(-1)^p f^{(p)}(1)=\sum_n \lambda_n^p a_n e^{-\lambda_n}$ 是正项收敛级数，从而正项双重级数

$$f(-\varepsilon)=\sum_{p,n} a_n \frac{1}{p!}(1+\varepsilon)^p \lambda_n^p e^{-\lambda_n}$$

收敛. 重新排列各项给出

$$f(-\varepsilon)=\sum_n a_n e^{-\lambda_n}\sum_{p=0}^{\infty}\frac{1}{p!}(1+\varepsilon)^p\lambda_n^p$$
$$=\sum_n a_n e^{-\lambda_n}e^{\lambda_n(1+\varepsilon)}=\sum_n a_n e^{\varepsilon\lambda_n},$$

这表明所给的 Dirichlet 级数对于 $z=-\varepsilon$ 收敛，从而对于 $\mathrm{Re}(z)>-\varepsilon$ 收敛。

2.4. 普通 Dirichlet 级数

这是情形 $\lambda_n=\log n$. 对应级数写成

$$f(s)=\sum_{n=1}^{\infty}a_n/n^s.$$

字母 s 已经成为该函数之自变量的传统符号.

命题 8 如果 a_n 有界，则 $f(s)$ 对于 $\mathrm{Re}(s)>1$ 绝对收敛.

证 这由熟知的 $\sum_{n=1}^{\infty}\frac{1}{n^\alpha}(\alpha>1)$ 收敛性质推出.

命题 9 如果部分和 $A_{m,p}=\sum_{n=m}^{p}a_n$ 有界，则 $f(s)$ 对于 $\mathrm{Re}(s)>0$ 收敛(不一定绝对收敛).

证 假设 $|A_{m,p}|\leqslant K$. 利用 Abel 引理(引理 2)，我们发现

$$|S_{m,m'}|\leqslant K\left(\sum_{n=m}^{m'-1}\left|\frac{1}{n^s}-\frac{1}{(n+1)^s}\right|+\left|\frac{1}{m'^s}\right|\right).$$

根据命题 6 可设 s 为实数，这使我们可以把上面不等式写成简单形式:

$$|S_{m,m'}|\leqslant K/m^s,$$

于是收敛性便成为显然的了.

§3. Zeta 函数和 L 函数

3.1. Euler 乘积

定义 2 函数 f: **N**→**C** 叫作积性函数，如果当 $(m, n)=1$

时，有 $f(mn)=f(m)f(n)$.

【例】 Euler 函数（第一章§1.2）和 Ramanujan 函数（第七章§4.5）都是积性函数.

设 f 是有界积性函数.

引理 4 Dirichlet 级数 $\sum_{n=1}^{\infty} f(n)/n^s$ 对于 $\mathrm{Re}(s)>1$ 绝对收敛，并且它在这个区域中的和等于收敛的无穷乘积

$$\prod_{p\in P}(1+f(p)p^{-s}+\cdots+f(p^m)p^{-ms}+\cdots).$$

（此处及以后我们以 P 表示全体素数所成的集合.）

证 级数的绝对收敛性是由于 f 的有界性（命题 8）. 命 S 为素数的有限集合，而命

$$\mathbf{N}(S)=\{n\geqslant 1 \mid n \text{ 为整数}, n \text{ 的素因子均属于 } S\}.$$

易知有下面的等式：

$$\sum_{n\in\mathbf{N}(S)} f(n)/n^s=\prod_{p\in S}\left(\sum_{m=0}^{\infty} f(p^m)/p^{ms}\right).$$

当 S 增大时，等式左边趋于 $\sum_{n=1}^{\infty} f(n)/n^s$，由此即知无穷乘积是收敛的，并且其值等于 $\sum f(n)/n^s$.

引理 5 如果 f 是完全积性的（即对任何 $n, n'\in\mathbf{N}$ 均有 $f(nn')=f(n)f(n')$），我们有

$$\sum_{n=1}^{\infty} f(n)/n^s=\prod_{p\in P}\frac{1}{1-f(p)p^{-s}}.$$

证 由上引理及等式 $f(p^m)=f(p)^m$ 推出.

3.2. Zeta 函数

将前节结果用于 $f=1$，我们得到函数

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_{p\in P}\frac{1}{1-\dfrac{1}{p^s}}.$$

这些公式对于 $\mathrm{Re}(s)>1$ 有意义，叫作 zeta 函数.

命题 10 (a) zeta 函数在半平面 $\mathrm{Re}(s)>1$ 中是全纯的，并且 $\neq 0$.

(b) $\zeta(s)=\dfrac{1}{s-1}+\phi(s)$，其中 $\phi(s)$ 为 $\mathrm{Re}(s)>0$ 中全纯函数.

证 (a)是显然的. 对于(b)，我们注意

$$\frac{1}{s-1}=\int_1^\infty t^{-s}dt=\sum_{n=1}^\infty\int_n^{n+1}t^{-s}dt,$$

从而

$$\zeta(s)=\frac{1}{s-1}+\sum_{n=1}^\infty\left(\frac{1}{n^s}-\int_n^{n+1}t^{-s}dt\right)$$

$$=\frac{1}{s-1}+\sum_{n=1}^\infty\int_n^{n+1}(n^{-s}-t^{-s})dt.$$

现在令

$$\phi_n(s)=\int_n^{n+1}(n^{-s}-t^{-s})dt,\qquad \phi(s)=\sum_{n=1}^\infty\phi_n(s).$$

我们必需证明 $\phi(s)$ 在 $\mathrm{Re}(s)>0$ 中是可定义的并且是全纯的. 但是显然每个 $\phi_n(s)$ 有这些性质，因此只需再证明级数 $\sum\phi_n$ 在 $\mathrm{Re}(s)>0$ 的每个紧集上均正则(*)收敛. 我们有

$$|\phi_n(s)|\leqslant\sup_{n\leqslant t\leqslant n+1}|n^{-s}-t^{-s}|.$$

但是函数 $n^{-s}-t^{-s}$ 的微商等于 s/t^{s+1}. 由此我们得到

$$|\phi_n(s)|\leqslant\frac{|s|}{n^{x+1}},\quad 其中\quad x=\mathrm{Re}(s).$$

从而对于每个 $\varepsilon>0$，级数 $\sum\phi_n$ 在 $\mathrm{Re}(s)\geqslant\varepsilon$ 中都正则收敛.

系 1 zeta 函数在 $s=1$ 有单极点.

(*) 对于函数级数 $\sum_{i=1}^\infty u_i(x)$，如果存在正数 a_i，使得 $|u_i(x)|\leqslant a_i(i=1, 2, \cdots)$ 并且 $\sum_{i=1}^\infty a_i$ 收敛，就称 $\sum_{i=1}^\infty u_i(x)$ 为正则收敛(normally covergent).

——译者注

这是显然的事实.

系 2 当 $s\to1$ 时,

$$\sum_p p^{-s}\sim\log\frac{1}{s-1},\quad 而\quad \sum_{p,k\geqslant2}\frac{1}{p^{ks}}$$

仍旧是有界的.

证 我们有

$$\log\zeta(s)=\sum_{p\in P,k\geqslant1}\frac{1}{kp^{ks}}=\sum_{p\in P}\frac{1}{p^s}+\psi(s),$$

其中 $\psi(s)=\sum_{p\in P}\sum_{k\geqslant2}\frac{1}{kp^{ks}}$. 级数 ψ 由

$$\sum_{p\in P,k\geqslant2}\frac{1}{p^{ks}}=\sum_p\frac{1}{p^s(p^s-1)}\leqslant\sum_p\frac{1}{p(p-1)}$$
$$\leqslant\sum_{n=2}^{\infty}\frac{1}{n(n-1)}=1$$

所控制. 由此推得 ψ 是有界的, 又由系 1 证得

$$\log\zeta(s)\sim\log\frac{1}{s-1},$$

从而得到系 2.

注 我们要提一下, $\zeta(s)$ 可以扩充成整个 **C** 上的亚纯函数, 并且在 $s=1$ 处有单极点, 虽然我们以后并不需要这一事实. 函数

$$\xi(s)=\frac{1}{2}s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

是全纯函数, 并且满足函数方程 $\xi(s)=\xi(1-s)$.

此外, zeta 函数在负整数处取有理值:

$$\zeta(-2n)=0,\qquad \zeta(1-2n)=(-1)^nB_n/2n\quad(n>0),$$

其中 B_n 为第 n 个 Bernoulli 数(见第七章 § 4.1).

猜想 ζ 的其他零点均在直线 $\mathrm{Re}(s)=\frac{1}{2}$ 上 (Riemann 猜

想)．已经对许多零点(多于三百万个)在数值上验证了这个猜想是对的．

3.3. L 函数

设 $m\geqslant 1$ 为整数，χ 为 mod m 特征(见 § 1.3)．对应的 L 函数定义成 Dirichlet 级数

$$L(s,\ \chi)=\sum_{n=1}^{\infty}\chi(n)n^{-s}.$$

注意在这个和式中，只有与 m 互素的 n 才给出非零的贡献．

对于单位特征的情形，本质上没有给出新的东西：

命题 11 对于 $\chi=1$ 我们有

$L(s,\ 1)=F(s)\zeta(s)$, 其中 $F(s)=\prod_{p|m}(1-p^{-s})$.

特别地，$L(s,\ 1)$ 可解析开拓到 $\mathrm{Re}(s)>0$，并且在 $s=1$ 有单极点．

证 这是显然的．

命题 12 对于 $\chi\neq 1$，级数 $L(s,\ \chi)$ 在半平面 $\mathrm{Re}(s)>0$ 中收敛，并且在 $\mathrm{Re}(s)>1$ 中绝对收敛．对于 $\mathrm{Re}(s)>1$ 我们有

$$L(s,\ \chi)=\prod_{p\in P}\frac{1}{1-\dfrac{\chi(p)}{p^s}}.$$

证 关于 $\mathrm{Re}(s)>1$ 的论断由 § 3.1 所述即可推得．剩下要证对于 $\mathrm{Re}(s)>0$ 级数是收敛的．由于命题 9，只需证和式

$$A_{u,v}=\sum_{n=u}^{v}\chi(n)\quad (u\leqslant v)$$

是有界的．现在根据命题 4 我们有

$$\sum_{n=u}^{u+m-1}\chi(n)=0.$$

从而只需对 $v-u<m$ 估计和式 $A_{u,v}$. 但显然有

$$|A_{u,v}|\leqslant\phi(m).$$

从而命题得证.

注 特别当 $\chi\neq1$ 时, $L(1,\ \chi)$ 是有限的. Dirichlet 证明的本质部分是要证明 $L(1,\ \chi)\neq0$, 这是下一节的内容.

3.4. 对于同一整数 m 的所有 L 函数之乘积

在本节中 $m\geqslant1$ 是固定的整数. 如果 $p\nmid m$, 我们以 $\bar{p}$ 表示它在 $G(m)=(\mathbf{Z}/m\mathbf{Z})^*$ 中的象, 而 $\bar{p}$ 在群 $G(m)$ 中的阶数用 $f(p)$ 表示. 根据定义, $f(p)$ 是满足 $p^f\equiv1\pmod m$ 的最小整数 $f>1$. 令

$$g(p)=\phi(m)/f(p).$$

这是 $G(m)$ 对于由 $\bar{p}$ 生成的子群 $(\bar{p})$ 之商群的阶数.

引理 6 如果 $p\nmid m$, 则有恒等式

$$\prod(1-\chi(p)T)=(1-T^{f(p)})^{g(p)},$$

其中乘积遍取 $G(m)$ 的全部特征 χ.

证 设 W 为 $f(p)$ 次单位根集合, 我们有恒等式

$$\prod_{w\in W}(1-wT)=1-T^{f(p)}.$$

由此以及对于每个 $w\in W$, 均有 $G(m)$ 的 $g(p)$ 个特征 χ 使 $\chi(\bar{p})=w$, 就可推出引理 6.

现在我们定义新的函数 $\zeta_m(s)$:

$$\zeta_m(s)=\prod_{\chi}L(s,\ \chi),$$

其中乘积遍取过 $G(m)$ 的所有特征 χ.

命题 13 $\zeta_m(s)=\prod_{p\nmid m}\dfrac{1}{\left(1-\dfrac{1}{p^{f(p)s}}\right)^{g(p)}}.$

这是具有正整系数的 Dirichlet 级数，并且在半平面 $\mathrm{Re}(s)>1$ 中收敛.

证 将每个 L 函数代之以它的乘积展开式，然后利用引理 6(取 $T=p^{-s}$)，我们得到 $\zeta_m(s)$ 的上述乘积展开式. 由这个展开式明显看出它的级数具有正整系数. 它在 $\mathrm{Re}(s)>1$ 中收敛则是显然的.

定理 1 (a) $\zeta_m(s)$ 在 $s=1$ 有单极点.

(b) 对于每个 $\chi\neq 1$, $L(1,\chi)\neq 0$.

证 如果 $\chi\neq 1$ 时 $L(1,\chi)\neq 0$，那末 $L(s,1)$ 在 $s=1$ 有单极点这一事实表明 ζ_m 在 $s=1$ 也有一单极点，因此 (b)⇒(a). 现在设对某个 $\chi\neq 1$ 有 $L(1,\chi)=0$，则函数 ζ_m 在 $s=1$ 处全纯，因此在 $\mathrm{Re}(s)>0$ 的每个 s 处都全纯(见命题 11 和命题 12). 由于它是具有正系数的 Dirichlet 级数，它在此区域的每点均收敛(命题 7). 但这是荒唐的，因为 ζ_m 的 p- 因子等于

$$\frac{1}{(1-p^{-f(p)s})^{g(p)}}=(1+p^{-f(p)s}+p^{-2f(p)s}+\cdots)^{g(p)},$$

它控制级数

$$1+p^{-\phi(m)s}+p^{-2\phi(m)s}+\cdots,$$

从而 ζ_m 的每个系数均大于级数

$$\sum_{(n,m)=1} n^{-\phi(m)s}$$

的相应的系数，而后一级数在 $s=\dfrac{1}{\phi(m)}$ 处发散. 这就完成了证明.

注 不计有限多个因子，函数 ζ_m 等于与 m 次单位根域相结合的 zeta 函数. ζ_m 在 $s=1$ 有单极点这一事实也可以从代数数域 zeta 函数的一般结果推出.

§4. 密度和 Dirichlet 定理

4.1. 密度

设 P 为素数集合，我们已经看到(命题 10 的系 2)，当 $s\to 1$ 时有

$$\sum_{p\in P}\frac{1}{p^s}\sim\log\frac{1}{s-1}.$$

设 A 为 P 的子集. 我们说 A 以实数 k 为密度，是指当 $s\to 1$ 时，比值

$$\left(\sum_{p\in A}\frac{1}{p^s}\right)\Big/\left(\log\frac{1}{s-1}\right)$$

趋于 k (当然这时有 $0\leqslant k\leqslant 1$). 关于算术级数的素数定理可以精密化成如下的形式:

定理 2 设 $m\geqslant 1$, 并设 a 适合 $(a, m)=1$,

$$P_a=\{p\in P\,|\,p\equiv a\pmod m\},$$

则集合 P_a 有密度 $1/\phi(m)$.

(换句话说，素数在 $\bmod m$ 不同的缩同余类中是"均匀分布"的.)

系 P_a 是无限集合.

这是因为有限集合的密度为零.

4.2. 一些引理

设 χ 是 $G(m)$ 的特征，令

$$f_\chi(s)=\sum_{p\nmid m}\chi(p)/p^s,$$

该级数当 $s>1$ 时收敛.

引理 7 如果 $\chi=1$, 则当 $s\to 1$ 时

$$f_\chi\sim\log\frac{1}{s-1}.$$

这是因为 f_1 与级数 $\sum \frac{1}{p^s}$ 只相差有限多项.

引理 8 如果 $\chi \neq 1$, 则当 $s \to 1$ 时 f_χ 保持为有界.

证 我们使用函数 $L(s, \chi)$ 的对数，但是它的意义必需说得更确切些(因为将 log 说成一个函数并不合适)：

$L(s, \chi)$ 由乘积 $\prod \frac{1}{1-\chi(p)p^{-s}}$ 所定义. 对于 $\operatorname{Re}(s)>1$, 每个因子均有形式 $\frac{1}{1-\alpha}$, 其中 $|\alpha|<1$. 我们定义 $\log \frac{1}{1-\alpha}$ 为 $\sum_{n=1} \frac{\alpha^n}{n}$, 然后定义 $\log L(s, \chi)$ 为级数：

$$\log L(s, \chi) = \sum \log \frac{1}{1-\chi(p)p^{-s}}$$

$$= \sum_{n,p} \frac{\chi(p)^n}{np^{ns}} \quad (\operatorname{Re}(s)>1),$$

这级数显然是收敛的. (一个等价的定义是：在 $\operatorname{Re}(s)>1$ 中取 $\log L(s, \chi)$ 的一个"分支"，使在实轴上当 $s \to +\infty$ 时，它变成零.)

现在将 $\log L(s, \chi)$ 拆成两部分：

$$\log L(s, \chi) = f_\chi(s) + F_\chi(s),$$

其中

$$F_\chi(s) = \sum_{p, n \geq 2} \frac{\chi(p)^n}{np^{ns}}.$$

定理 1 和命题 10 的系 2 表明 $\log L(s, \chi)$ 和 $F_\chi(s)$ 在 $s \to 1$ 时保持为有界. 从而 $f_\chi(s)$ 亦是如此，这就证明了引理.

4.3. 定理 2 的证明

我们必需研究函数

$$g_a(s) = \sum_{p \in P_a} \frac{1}{p^s}$$

在 $s \to 1$ 时的性状.

引理 9 $g_a(s)=\frac{1}{\phi(m)}\sum_{\chi}\chi(a)^{-1}f_{\chi}(s)$,

求和遍取 $G(m)$ 的所有特征 χ.

证 将 f_χ 用它的定义公式代入，函数 $\sum\chi(a)^{-1}f_\chi(s)$ 可以写成

$$\sum_{p\nmid m}\left(\sum_{\chi}\chi(a^{-1})\chi(p)\right)/p^s.$$

但是 $\chi(a^{-1})\chi(p)=\chi(a^{-1}p)$. 由命题 4 的系我们有

$$\sum_{\chi}\chi(a^{-1}p)=\begin{cases}\phi(m), & \text{如果 } a^{-1}p\equiv 1 \pmod m;\\ 0, & \text{否则}.\end{cases}$$

于是便得到函数 $\phi(m)g_a(s)$.

定理 2 现在显然. 事实上，引理 7 表明对于 $\chi=1$ 有

$$f_\chi(s)\sim\log\frac{1}{s-1}.$$

而引理 8 表明其余的 f_χ 均有界. 利用引理 9 我们看到

$$g_a(s)\sim\frac{1}{\phi(m)}\log\frac{1}{s-1},$$

这就意味着 P_a 的密度是 $\frac{1}{\phi(m)}$，证毕.

4.4. 一个应用

命题 14 设 a 为整数，并且不是平方数. 则满足

$$\left(\frac{a}{p}\right)=1$$

的素数 p 所成的集合有密度 1/2.

证 我们可设 a 是无平方因子的. 令 $m=4|a|$，χ_a 为 §1.3 命题 5 中所定义的 $\bmod m$ 特征，$H\subset G(m)$ 是 χ_a 在 $G(m)$ 中的核. 如果素数 p 与 m 互素，以 $\bar{p}$ 表示它在 $G(m)$ 中的象. 我们有 $\left(\frac{a}{p}\right)=1\Leftrightarrow\bar{p}\in H$. 根据定理 2，满足这个条件

的素数集合有密度 $1/(G:H)=1/2$.

系 设 a 为整数，如果方程 $X^2-a=0$ 对几乎所有的 $p\in P$ 均有 $\bmod p$ 解，则它在 $\mathbf{Z}$ 中也有解.

注 对于其他类型的一些方程也有类似结果，例如：

i) 设 $f(x)=a_0X^n+\cdots+a_n$ 是整系数 n 次多项式，并且在 $\mathbf{Q}$ 上不可约. 令 K 为由 f 的全体根生成的域（在 $\mathbf{Q}$ 之某个代数闭包中）. 又令 $N=[K:\mathbf{Q}]$. 我们有 $N\geqslant n$. 令

$$P_f=\{p\in P \mid f(\bmod p)\text{完全分解，即} f(\bmod p)\text{的根均}\in \mathbf{F}_p\}.$$

可以证明 P_f 有密度 $\frac{1}{N}$.（其证明方法与 Dirichlet 定理类似，使用域 K 的 zeta 函数在 $s=1$ 有单极点这一事实.）还可以给出集合

$$P'_f=\{p\in P \mid f\ (\bmod p)\text{的简化在 } \mathbf{F}_p \text{ 中至少有一根}\}$$

的密度. 其值为形如 q/N 的数，其中 $1\leqslant q<N$（除了平凡情形 $n=1$ 之外）.

ii) 更一般地，令 $\{f_\alpha(x_1,\cdots,x_n)\}$ 为一族整系数多项式，令

$$Q=\{p\in P \mid f_\alpha(\bmod p)\text{的简化在}(\mathbf{F}_p)^n\text{中有公共零点}\}.$$

可以证明(见 J. Ax, Ann. of Maths., 85, 1967, pp. 161～183)，Q 具有密度，其密度为有理数，并且只有当 Q 是有限集合时其密度才为零.

4.5. 自然密度

本节中所使用的密度叫作"解析密度"（或"Dirichlet 密度"）. 虽然它看起来复杂，但用起来却很方便.

还有另一个密度叫作"自然密度"：P 的子集合 A 叫作有自然密度 k，如果当 $n\to\infty$ 时比值

$$\frac{A\text{ 中}\leqslant n\text{ 的元素个数}}{P\text{ 中}\leqslant n\text{ 的元素个数}}$$

趋于 k.

可以证明，如果 A 有自然密度 k，则 A 的解析密度也存在并且等于 k. 另一方面，却存在着这样的集合，它有解析密度但是却没有自然密度. 例如集合

$$P^1=\{p\in P\,|\,p\text{(在十进制中)的个位是 }1\}$$

就是如此. 利用素数定理不难看出它没有自然密度，另一方面，Bombieri 给我看了一个 P^1 的解析密度是存在的证明(它等于 $\log_{10}2=0.3010300\cdots$).

但是，对于上面所考虑的素数集合是不会发生这种现象的：集合 $\{p\in P\,|\,p\equiv a\pmod m\}$ 有自然密度$\left(\text{当 }(a,\ m)=1\text{ 时它等于 }\frac{1}{\phi(m)}\right)$. 对于上一小节的集合 P_f, P'_f 和 Q 也是同样的. 证明(以及"误差项"的估计)见 K. Prachar: Primzahlverteilung, 第五章 § 7.

第七章　模　形　式

§1. 模　　群

1.1. 定义

令 H 表示 $\mathbf{C}$ 的上半平面，即集合 $\{z\in\mathbf{C}\mid \operatorname{Im}(z)>0\}$.

令 $\mathrm{SL}_2(\mathbf{R})$ 为群

$$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\middle|\, a,\ b,\ c,\ d\in\mathbf{R},\ ad-bc=1\right\}.$$

我们用下述方式将 $\mathrm{SL}_2(\mathbf{R})$ 作用在 $\tilde{\mathbf{C}}=\mathbf{C}\cup\{\infty\}$ 之上：

如果 $g=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\mathrm{SL}_2(\mathbf{R})$，$z\in\tilde{\mathbf{C}}$，我们令

$$gz=\frac{az+b}{cz+d}.$$

容易验证有公式

$$\operatorname{Im}(gz)=\frac{\operatorname{Im}(z)}{|cz+d|^2}. \tag{1}$$

这表明 H 在 $\mathrm{SL}_2(\mathbf{R})$ 的作用下仍旧是 H. 注意 $\mathrm{SL}_2(\mathbf{R})$ 中元素 $-1=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ 在 H 上作用平凡. 因此我们可以考虑作用群是 $\mathrm{PSL}_2(\mathbf{R})=\mathrm{SL}_2(\mathbf{R})/\{\pm 1\}$（这个群的作用是忠实的，甚至可以证明这是 H 的解析自同构群）.

设 $\mathrm{SL}_2(\mathbf{Z})$ 为整系数矩阵所组成的 $\mathrm{SL}_2(\mathbf{R})$ 的子群，它是 $\mathrm{SL}_2(\mathbf{R})$ 的离散子群.

定义 1　群 $G=\mathrm{SL}_2(\mathbf{Z})/\{\pm 1\}$ 叫作模群. 它是 $\mathrm{SL}_2(\mathbf{Z})$ 在 $\mathrm{PSL}_2(\mathbf{R})$ 中的象.

如果 $g\in\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 为 $\mathrm{SL}_2(\mathbf{Z})$ 中元素，我们常常用同一符号表示它在模群 G 中的象.

1.2. 模群的基本区域

设 $S=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, 它们均是 G 中元素. 我们有

$$Sz=-\frac{1}{z},\quad Tz=z+1,\quad S^2=1,\quad (ST)^3=1.$$

另一方面, 令

$$D=\{z\in H \mid |z|\geqslant 1,\ |\mathrm{Re}(z)|\leqslant 1/2\}.$$

下图画出了 D 被群 G 中元素

$$\{1,\ T,\ TS,\ ST^{-1}S,\ ST^{-1},\ S,\ ST,\ STS,\ T^{-1}S,\ T^{-1}\}$$

所变成的各区域.

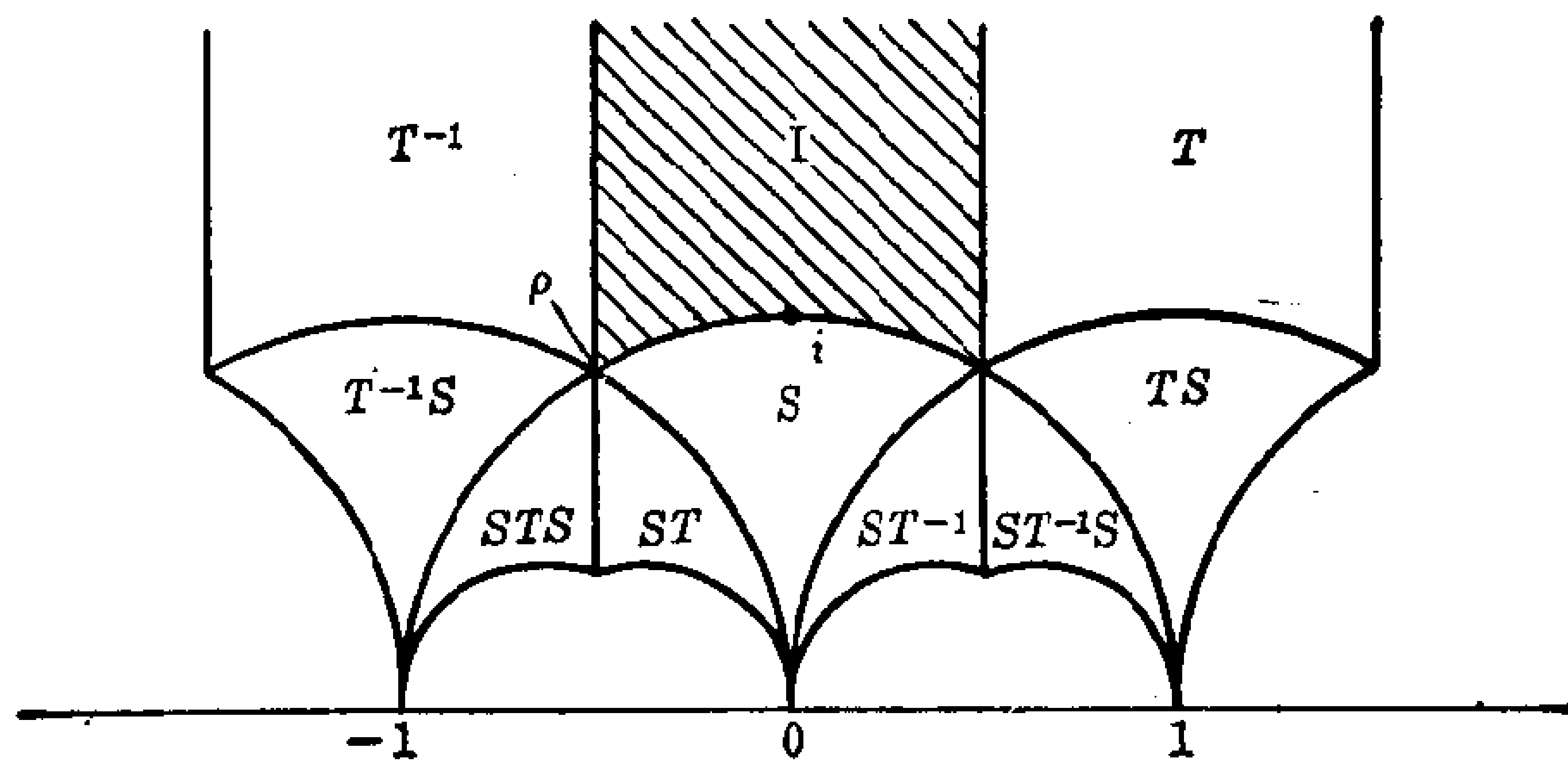


图 1

我们要证明 D 是 G 在半平面 H 上作用的基本区域. 更确切地说:

定理 1 (1) 对于每个 $z\in H$, 存在 $g\in G$, 使 $gz\in D$.

(2) 设 D 中两个不同的点 z 和 z' 是 mod G 共轭 (congruent)的，则或者 $\operatorname{Re}(z)=\pm\frac{1}{2}$ 并且 $z=z'\pm1$；或者 $|z|=1$ 并且 $z'=-\frac{1}{z}$.

(3) 令 $z\in D$, $I(z)=\{g\in G\,|\,gz=z\}$ 是 z 在 G 中的固定子群，则除了下述三种情形之外我们有 $I(z)=\{1\}$：

$z=i$，此时 $I(z)$ 是由 S 生成的二阶群.

$z=\rho=e^{2\pi i/3}$，此时 $I(z)$ 是由 ST 生成的三阶群.

$z=-\bar{\rho}=e^{\pi i/3}$，此时 $I(z)$ 是由 TS 生成的三阶群.

由(1)和(2)推出：

系 正则映射 $D\to H/G$ 是映上，并且它在 D 的内部的限制是单射.

定理 2 群 G 由 S 和 T 生成.

定理 1 和定理 2 的证明 令 G' 是由 S 和 T 生成的 G 之子群，$z\in H$. 我们要证明存在 $g'\in G'$ 使 $g'z\in D$，这就证明了定理 1 的论断(1). 如果

$$g=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in G',$$

则

$$\operatorname{Im}(gz)=\frac{\operatorname{Im}(z)}{|cz+d|^2}. \tag{1}$$

因为 c 和 d 是整数，从而使 $|cz+d|$ 小于一给定数的数对 (c,d) 只有有限多个. 这表明存在 $g\in G'$，使 $\operatorname{Im}(gz)$ 最大. 现在取整数 n，使 $T^n gz$ 的实部在 $-1/2$ 和 $1/2$ 之间. 元素 $z'=T^n gz$ 便属于 D. 事实上，这只需证明 $|z'|\geqslant1$. 如果 $|z'|<1$，则元素 $-1/z'$ 的虚部严格地大于 $\operatorname{Im}(z')$，而这是不可能的. 于是元素 $g'=T^n g$ 即有所需性质.

我们现在证明定理1中的(2)和(3). 令 $z\in D$, 而 $g=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in G$, 使 $gz\in D$. 必要时以 (gz, g^{-1}) 代替 (z, g), 我们可设 $\text{Im}(gz)\geqslant\text{Im}(z)$, 即 $|cz+d|\leqslant 1$. 如果 $|c|\geqslant 2$, 这显然是不可能的. 于是只剩下 $c=0$, ± 1 三种情形. 如果 $c=0$, 我们有 $d=\pm 1$, 而 g 是平移 $\pm b$. 因为 $\text{Re}(z)$ 和 $\text{Re}(gz)$ 均在 $-1/2$ 和 $1/2$ 之间, 从而或者 $b=0$ 并且 $g=1$; 或者 $b=\pm 1$. 对于后一种情形, $\text{Re}(z)$ 和 $\text{Re}(gz)$ 必然一为 $-1/2$, 一为 $1/2$. 如果 $c=1$, 则 $|z+d|\leqslant 1\Rightarrow d=0$, 除非 $z=\rho$ 或 $-\bar{\rho}$. 对于 $z=\rho$, 我们可以有 $d=0, 1$; 对于 $z=-\bar{\rho}$ 我们有 $d=0$, -1. 情形 $d=0$ 给出 $|z|\leqslant 1$, 于是 $|z|=1$. 另一方面, $ad-bc=1$ 导致 $b=-1$, 从而 $gz=a-1/z$. 而在证明(1)的过程中推出 $a=0$, 除非 $\text{Re}(z)=\pm\frac{1}{2}$, 即除非 $z=\rho$ 或 $-\bar{\rho}$. 当 $z=\rho$ 时我们有 $a=0$, -1; 当 $z=-\bar{\rho}$ 时则有 $a=0$, $+1$. 情形 $z=\rho$, $d=1$ 给出 $a-b=1$ 和 $g\rho=a-\frac{1}{1+\rho}=a+\rho$, 从而 $a=0$, 1. 情形 $z=-\bar{\rho}$, $d=-1$ 给出类似论断. 最后, 情形 $c=-1$ 在 a, b, c, d 均改变符号时(此时 g 不变)可以化为情形 $c=1$. 这就证明了论断(2)和(3)的正确性.

剩下要证 $G'=G$. 令 $g\in G$, 取 z_0 为 D 之内点(例如取 $z_0=2i$), 令 $z=gz_0$. 我们从上面已经知道, 存在 $g'\in G'$ 使 $g'z\in D$. D 中两点 z_0 和 $g'z=g'gz_0$ 是 $\text{mod}\, G$ 共轭的, 并且它们当中有一个是 D 之内点. 根据(2)和(3), 即知这二点是同一点, 于是 $g'g=1$, 即 $g\in G'$. 这就完成了证明.

注 可以证明 $\langle S, T \mid S^2=(ST)^3=1\rangle$ 是群 G 的表现(presentation), 或者等价地说成 G 是由 S 生成的二阶循环群和 ST 生成的3阶循环群的自由积.

§2. 模 函 数

2.1. 定义

定义 2 设 k 是整数. 我们称函数 f 是权为 $2k$[注]的弱模函数，如果 f 在半平面 H 上亚纯并且有如下的关系式：

(2)
$$f(z)=(cz+d)^{-2k}f\left(\frac{az+b}{cz+d}\right),$$
$$\text{对一切}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in \mathrm{SL}_2(\mathbf{Z}).$$

设 g 是 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 在 G 中的象，我们有

$$\frac{d(gz)}{dz}=(cz+d)^{-2},$$

于是关系(2)可以写成

$$\frac{f(gz)}{f(z)}=\left(\frac{d(gz)}{dz}\right)^{-k},$$

或者

(3)
$$f(gz)d(gz)^k=f(z)dz^k.$$

这意味着"权 k 的微分型"$f(z)dz^k$ 在 G 下不变. 因为 G 是由元素 S 和 T 生成的(见定理 2)，这只需对 S 和 T 检查不变性即可. 于是给出：

命题 1 设函数 f 在 H 上亚纯. 则函数 f 是权 $2k$ 的弱模函数的充要条件是它满足下面两个条件：

(4)
$$f(z+1)=f(z),$$

(5)
$$f\left(-\frac{1}{z}\right)=z^{2k}f(z).$$

假若关系式(4)成立，我们可以将 f 表示成 $q=e^{2\pi iz}$ 的函

[注] 有些作者称 f 是"权为 $-2k$ 的"或"权为 k 的".

数，这个函数记成 $\tilde{f}$，它是圆盘 $|q|<1$（去掉原点）中的亚纯函数．如果 $\tilde{f}$ 可扩充成在原点的亚纯函数（或全纯函数），我们便称 f 在 ∞ 处亚纯（或全纯）．这意味着 $\tilde{f}$ 在原点某邻域中有 Laurent 展开

$$\tilde{f}(q)=\sum_{n=-\infty}^{+\infty} a_n q^n,$$

其中对于充分小的 n（或对于 $n<0$），a_n 为 0.

定义 3 一个弱模函数如果在 ∞ 处亚纯，就称作是模函数.

如果 f 在 ∞ 处全纯，我们令 $f(\infty)=\tilde{f}(0)$，这便是 f 在 ∞ 处的值.

定义 4 处处（包括 ∞）全纯的模函数称为模形式．如果这样一个函数在 ∞ 处是 0，便称为 cusp 型．（cusp form，德文 Spitzenform，法文 forme parabolique.）

于是，权 $2k$ 的模形式由级数

$$f(z)=\sum_{n=0}^{\infty} a_n q^n=\sum_{n=0}^{\infty} a_n e^{2\pi inz} \tag{6}$$

给出，它对于 $|q|<1$（即 $\mathrm{Im}(z)>0$）收敛，且有恒等式

$$f\left(-\frac{1}{z}\right)=z^{2k}f(z). \tag{5}$$

如果 $a_0=0$，它便是 cusp 型.

【例】 1）如果 f 和 f' 是权 $2k$ 和 $2k'$ 的模形式，则乘积 ff' 是权 $2k+2k'$ 的模形式.

2）我们以后将看到，函数

$$q\prod_{n=1}^{\infty}(1-q^n)^{24}=q-24q^2+252q^3-1472q^4+\cdots$$

是权 12 的 cusp 型.

2.2. 格函数和模函数

我们先回忆一下什么是有限维实向量空间 V 中的格. 这是 V 的一个子群 Γ, Γ 满足下面几个彼此等价的条件之一:

i) Γ 离散并且 V/Γ 紧;

ii) Γ 离散并且生成 $\mathbf{R}$-向量空间 V;

iii) 存在 V 的 $\mathbf{R}$-基 $(e_1, \cdots, e_n)$, 它是 Γ 的 $\mathbf{Z}$-基(即 $\Gamma=\mathbf{Z}e_1\oplus\cdots\oplus\mathbf{Z}e_n$).

设 $\mathscr{R}$ 是 $\mathbf{C}$ (看作 $\mathbf{R}$-向量空间) 的全部格所构成之集合. 令

$$M=\{(\omega_1, \omega_2)\in(\mathbf{C}^*)^2 \mid \operatorname{Im}(\omega_1/\omega_2)>0\}.$$

对于每个 $(\omega_1, \omega_2)\in M$, 我们结合一个以 $\{\omega_1, \omega_2\}$ 为基的格

$$\Gamma(\omega_1, \omega_2)=\mathbf{Z}\omega_1\oplus\mathbf{Z}\omega_2.$$

于是我们得到一个映射 $M\to\mathscr{R}$, 它显然是映上.

令 $$g=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in \mathrm{SL}_2(\mathbf{Z}), \quad (\omega_1, \omega_2)\in M.$$

我们令 $$\omega_1'=a\omega_1+b\omega_2, \quad \omega_2'=c\omega_1+d\omega_2.$$

显然 $\{\omega_1', \omega_2'\}$ 也是 $\Gamma(\omega_1, \omega_2)$ 的基. 而且若令

$$z=\omega_1/\omega_2, \quad z'=\omega_1'/\omega_2',$$

我们有 $$z'=\frac{az+b}{cz+d}=gz.$$

这证明 $\operatorname{Im}(z')>0$, 从而 $(\omega_1', \omega_2')\in M$.

命题 2 M 中两个元素定义同一个格的充要条件是它们 $\bmod\, \mathrm{SL}_2(\mathbf{Z})$ 共轭.

证 我们刚才看到条件是充分的. 反之, 如果 (ω_1, ω_2) 和 $(\omega_1', \omega_2')\in M$, 它们定义同一个格, 则存在行列式为 ±1 的整系数矩阵 $g=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, 它将第一组基变成第二组基. 如果 $\det(g)<0$, 直接计算可知 $\operatorname{Im}(\omega_1'/\omega_2')$ 的符号与 $\operatorname{Im}(\omega_1/\omega_2)$ 的

符号相反．因此若它们的符号相同，必然 $\det(g)=1$，这就证明了命题．

于是我们可以把 $\mathbf{C}$ 的格集合 $\mathscr{R}$ 等同于 M 被 $\mathrm{SL}_2(\mathbf{Z})$ 作用的商集．

现在由

$$\Gamma \mapsto \lambda\Gamma \quad 和 \quad (\omega_1, \omega_2) \mapsto (\lambda\omega_1, \lambda\omega_2), \qquad \lambda \in \mathbf{C}^*$$

将 $\mathbf{C}^*$ 作用于 $\mathscr{R}$ 和 M 上．由 $(\omega_1, \omega_2) \mapsto z=\omega_1/\omega_2$ 将商 $M/\mathbf{C}^*$ 等同于 H，这个等同将 $\mathrm{SL}_2(\mathbf{Z})$ 在 M 上的作用转变成 $G=\mathrm{SL}_2(\mathbf{Z})/\{\pm 1\}$ 在 H 上的作用(见§1.1)．从而

命题 3 映射 $(\omega_1, \omega_2) \mapsto \omega_1/\omega_2$ 转到商集合之后，给出 $\mathscr{R}/\mathbf{C}^*$ 到 H/G 上的一一映射．(因此，H/G 中元素不计相似(homothety)等同于 $\mathbf{C}$ 的一个格．)

注 让我们将 $\mathbf{C}$ 的格 Γ 结合一个椭圆曲线 $E_\Gamma=\mathbf{C}/\Gamma$．易知两个格 Γ 和 Γ' 定义出同构的椭圆曲线，其充要条件是它们为相似的格．这就给出 $H/G=\mathscr{R}/\mathbf{C}^*$ 的第三个刻划方式：它是椭圆曲线同构类集合．

现在让我们转到模函数上来．设 F 是 $\mathscr{R}$ 上函数，取值于 $\mathbf{C}$．令 $k\in\mathbf{Z}$．我们称 F 是权为 $2k$ 的是指对于每个格 Γ 和 $\lambda\in\mathbf{C}^*$ 均有

$$F(\lambda\Gamma)=\lambda^{-2k}F(\Gamma). \tag{7}$$

设 F 是这样一个函数．如果 $(\omega_1, \omega_2)\in M$，我们以 $F(\omega_1, \omega_2)$ 表示 F 在格 $\Gamma(\omega_1, \omega_2)$ 上的值．公式(7)就变成

$$F(\lambda\omega_1, \lambda\omega_2)=\lambda^{-2k}F(\omega_1, \omega_2). \tag{8}$$

而且 $F(\omega_1, \omega_2)$ 在 $\mathrm{SL}_2(\mathbf{Z})$ 对 M 的作用下是不变的．

公式(8)表示乘积 $\omega_2^{2k}F(\omega_1, \omega_2)$ 只依赖于 $z=\omega_1/\omega_2$．于是存在 H 上函数 f，使得

$$F(\omega_1, \omega_2)=\omega_2^{-2k}f(\omega_1/\omega_2). \tag{9}$$

写下 F 在 $\mathrm{SL}_2(\mathbf{Z})$ 下不变，我们看到 f 满足恒等式：

$$f(z)=(cz+d)^{-2k}f\left(\frac{az+b}{cz+d}\right), \tag{2}$$

$$\text{对一切}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in \mathrm{SL}_2(\mathbf{Z}).$$

反之，如果 f 满足(2)式，则由公式(9)给出与 f 相结合的 $\mathscr{R}$ 上函数 F，F 是权 $2k$ 的函数．因此，我们可以把权 $2k$ 的模函数等同于权 $2k$ 的某个格函数．

2.3．模函数的例子；Eisenstein 级数

引理 1 设 Γ 为 $\mathbf{C}$ 中格．则级数 $\sum\limits_{\gamma\in\Gamma}' \frac{1}{|\gamma|^\sigma}$ 当 $\sigma>2$ 时收敛．

（符号 Σ' 表示求和遍取 Γ 的非零元素．）

证 我们可以象处理级数 $\sum 1/n^\alpha$ 那样去做，即通过考虑二重积分 $\iint\frac{dxdy}{(x^2+y^2)^{\sigma/2}}$（积分区域是中心在 0 的平面圆盘）来控制引理中的级数，利用极坐标很容易计算这个二重积分．另一个本质上等价的方法是，注意到 Γ 中使 $|\gamma|$ 在两个相邻整数 n 和 $n+1$ 之间的元素个数是 $O(n)$，因此引理中级数的收敛性归结为级数 $\sum 1/n^{\sigma-1}$ 的收敛性．

现在令 $k>1$ 为整数．如果 Γ 是 $\mathbf{C}$ 的格，令

$$G_k(\Gamma)=\sum_{\gamma\in\Gamma}' 1/\gamma^{2k}. \tag{10}$$

根据引理 1，这个级数是绝对收敛的．显然 G_k 是权 $2k$ 的函数，称作是指标为 k（有些作者称作是指标为 $2k$）的 Eisenstein 级数．象前一节那样，我们可以把 G_k 看作是 M 上的函数：

$$G_k(\omega_1,\ \omega_2)=\sum_{m,n}' \frac{1}{(m\omega_1+n\omega_2)^{2k}}. \tag{11}$$

这里符号 $\sum'$ 表示求和遍取全部不等于 (0, 0) 的整数对 (m, n). H 上对应于 G_k 的函数(由前一节所给出的)仍旧记为 G_k. 根据公式(9)和(11)我们有

$$G_k(z)=\sum_{m,n}'\frac{1}{(mz+n)^{2k}}. \tag{12}$$

命题 4 设 $k>1$ 为整数. 则 Eisenstein 级数 $G_k(z)$ 是权 $2k$ 的模形式. 我们有 $G_k(\infty)=2\zeta(2k)$, 其中 ζ 是 Riemann zeta 函数.

证 上面的推理已经表明 $G_k(z)$ 是权 $2k$ 的弱模形式. 我们还必需证明 G_k 处处(包括 ∞)全纯. 设 $z\in D$(见 § 1.2), 则

$$\begin{aligned}|mz+n|^2&=m^2z\bar{z}+2mn\,\mathrm{Re}(z)+n^2\geqslant m^2-mn+n^2\\&=|m\rho-n|^2.\end{aligned}$$

根据引理 1, 级数 $\sum'\frac{1}{|m\rho-n|^{2k}}$ 收敛. 这表明级数 $G_k(z)$ 在 D 中正则收敛, 将此结果用于 $G_k(g^{-1}z)$, $g\in G$, 即知在每个 gD 中, $G_k(z)$ 也正则收敛. 因为它们覆盖 H(定理 1), 因此 G_k 在 H 中全纯. 剩下要证 G_k 在 ∞ 处也全纯(并且求出它在 ∞ 的值). 这只要证明 G_k 在 $\mathrm{Im}(z)\to\infty$ 时有极限即可. 然而我们仍可设 z 在基本区域 D 中. 由于在 D 中的一致收敛性, 我们可以逐项取极限. $1/(mz+n)^{2k}$ 这一项当 $m\neq 0$ 时给出 0, $m=0$ 时给出 $1/n^{2k}$. 因此

$$\lim G_k(z)=\sum'\frac{1}{n^{2k}}=2\sum_{n=1}^{\infty}\frac{1}{n^{2k}}=2\zeta(2k).$$

证毕.

注 在下面 § 4.2 中我们将给出 G_k 展成 $q=e^{2\pi iz}$ 的幂级数展开式.

【例】 权数最小的 Eisenstein 级数是 G_2 和 G_3, 它们的

权分别为 4 和 6. 通常(由于椭圆曲线理论)它们代之以:

$$g_2=60G_2,\quad g_3=140G_3. \tag{13}$$

我们有 $g_2(\infty)=120\zeta(4)$, $g_3(\infty)=280\zeta(6)$. 利用已知的值 $\zeta(4)$ 和 $\zeta(6)$ (例如见下面 § 4.1), 我们发现

$$g_2(\infty)=\frac{4}{3}\pi^4,\quad g_3(\infty)=\frac{8}{27}\pi^6. \tag{14}$$

如果我们令

$$\Delta=g_2^3-27g_3^2, \tag{15}$$

便有 $\Delta(\infty)=0$. 这就是说, Δ 是权 12 的 cusp 型.

与椭圆曲线的关系

设 Γ 是 $\mathbf{C}$ 的格, 并令

$$\wp_\Gamma(u)=\frac{1}{u^2}+\sum_{\gamma\in\Gamma}{}'\left(\frac{1}{(u-\gamma)^2}-\frac{1}{\gamma^2}\right) \tag{16}$$

是对应的 Weierstrass 函数[注]. $G_k(\Gamma)$ 出现在 $\wp_\Gamma$ 的 Laurent 展开式中:

$$\wp_\Gamma(u)=\frac{1}{u^2}+\sum_{k=2}^{\infty}(2k-1)G_k(\Gamma)u^{2k-2}. \tag{17}$$

如果令 $x=\wp_\Gamma(u)$, $y=\wp'_\Gamma(u)$, 我们有

$$y^2=4x^3-g_2x-g_3, \tag{18}$$

其中 $g_2=60G_2(\Gamma)$, $g_3=140G_3(\Gamma)$ 如上所示. $\Delta=g_2^3-27g_3^2$ 与多项式 $4x^3-g_2x-g_3$ 的判别式只相差一个常数因子.

可以证明, 在射影平面中由方程(18)所定义的三次曲线同构于椭圆曲线 $\mathbf{C}/\Gamma$. 特别地, 它是非奇异曲线, 这就表明 $\Delta\neq0$.

[注] 例如见 H. Cartan,单复变量或多复变量解析函数的初等理论,第 V 章 § 2, n°5. (英译本: Addison-Wesley 公司.)

§3. 模形式空间

3.1. 模函数的零点和极点

设 f 是 H 上不恒等于零的亚纯函数，而 p 是 H 中一点. 使 $f/(z-p)^n$ 在 p 处全纯且不为零的整数 n 称作是 f 在点 p 的阶，记为 $v_p(f)$.

如果 f 是权为 $2k$ 的模函数，恒等式

$$f(z)=(cz+d)^{-2k}f\left(\frac{az+b}{cz+d}\right)$$

表明当 $g\in G$ 时，$v_p(f)=v_{g(p)}(f)$. 换句话说，$v_p(f)$ 只依赖于 p 在 H/G 中的象. 此外，我们可定义 $v_\infty(f)$ 为与 f 相结合的函数 $\tilde{f}$(见 § 2.1)在 $q=0$ 的阶.

最后，我们以 e_p 表示点 p 的固定子群的阶数. 如果 $p \bmod G$ 共轭于 i 或 ρ，则 e_p 分别等于 2 或 3，否则有 $e_p=1$，见定理 1.

定理 3 设 f 是权 $2k$ 的不恒为零的模函数，则

$$v_\infty(f)+\sum_{p\in H/G}\frac{1}{e_p}v_p(f)=\frac{k}{6}. \tag{19}$$

[我们还可以把这个公式写成

$$v_\infty(f)+\frac{1}{2}v_i(f)+\frac{1}{3}v_\rho(f)+\sum_{p\in H/G}^{*}v_p(f)=\frac{k}{6}. \tag{20}$$

其中符号 Σ^* 表示求和遍取 H/G 中不属于 i 和 ρ 之共轭类的那些点.]

证 首先注意定理 3 中所写的和式是有意义的，即 $f \bmod G$ 只有有限个零点与极点. 事实上，因为 $\tilde{f}$ 亚纯，从而存在 $r>0$，使 $\tilde{f}$ 在 $0<|q|<r$ 时既没有零点又没有极点. 这表示 f 在 $\mathrm{Im}(z)>e^{2\pi r}$ 中既没有零点又没有极点. 现在，基本区域 D 中由不等式 $\mathrm{Im}(z)\leqslant e^{2\pi r}$ 所定义的部分 D_r 是紧集. 因

为 f 在 H 中亚纯，它在 D_r 中只有有限多个零点和极点，这就是我们的论断.

为了证明定理3，我们要在 D 的边界上对 $\frac{1}{2\pi i}\frac{df}{f}$ 积分. 更确切地说:

1) 设 f 在 D 的边界上可能除了 i, ρ 和 $-\bar{\rho}$ 之外没有零点与极点，则存在着如图 2 所示的围道 $\mathscr{C}$，其内部包含 f 之每个不共轭于 i 或 ρ 的零点和极点的一个代表点. 由残数定理我们有

$$\frac{1}{2\pi i}\int_{\mathscr{C}}\frac{df}{f}=\sum_{p\in H/G}^{*}v_p(f).$$

另一方面:

a) 变量代换 $q=e^{2\pi iz}$ 把弧 EA 变成中心在 $q=0$ 的圆周 ω (具有负方向)，并且可能除了 0 之外不包含 $\tilde{f}$ 的任何零点与极点. 于是

$$\frac{1}{2\pi i}\int_E^A\frac{df}{f}=\frac{1}{2\pi i}\int_\omega\frac{df}{f}=-v_\infty(f).$$

b) 在包含弧 BB' 的圆周上(沿负方向)对 $\frac{1}{2\pi i}\frac{df}{f}$ 积分，其值为 $-v_\rho(f)$. 如果此圆周半径趋于 0，则角 $\widehat{BB'}$ 趋于 $\frac{2\pi}{6}$. 于是

$$\frac{1}{2\pi i}\int_B^{B'}\frac{df}{f}\to-\frac{1}{6}v_\rho(f).$$

类似地当弧 CC' 和 DD' 的半径趋于 0 时:

$$\frac{1}{2\pi i}\int_C^{C'}\frac{df}{f}\to-\frac{1}{2}v_i(f),$$

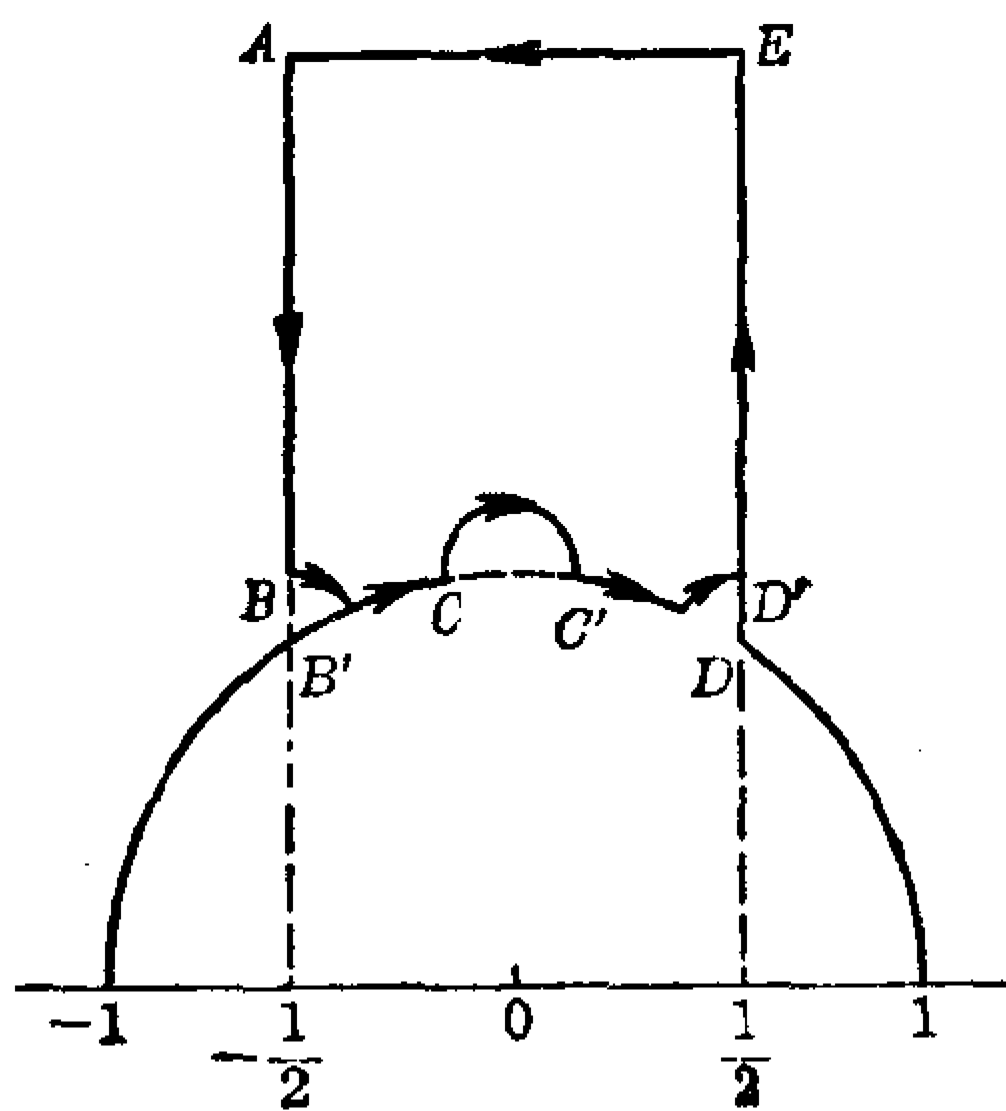


图 2

$$\frac{1}{2\pi i}\int_{D}^{D'}\frac{df}{f}\to-\frac{1}{6}v_\rho(f).$$

c) T 将弧 AB 变成弧 ED'. 由于 $f(Tz)=f(z)$, 我们得到

$$\frac{1}{2\pi i}\int_{A}^{B}\frac{df}{f}+\frac{1}{2\pi i}\int_{D'}^{E}\frac{df}{f}=0.$$

d) S 将弧 $B'C$ 变成弧 DC'. 由于 $f(Sz)=z^{2k}f(z)$, 我们得到

$$\frac{df(Sz)}{f(Sz)}=2k\frac{dz}{z}+\frac{df(z)}{f(z)}.$$

于是当弧 BB', CC' 和 DD' 的半径均趋于0时,

$$\frac{1}{2\pi i}\int_{B'}^{C}\frac{df}{f}+\frac{1}{2\pi i}\int_{C'}^{D}\frac{df}{f}=\frac{1}{2\pi i}\int_{B'}^{C}\left(\frac{df(z)}{f(z)}-\frac{df(Sz)}{f(Sz)}\right)$$
$$=\frac{1}{2\pi i}\int_{B'}^{C}\left(-2k\frac{dz}{z}\right)\to-2k\left(-\frac{1}{12}\right)=\frac{k}{6}.$$

现在写下我们给出的 $\frac{1}{2\pi i}\int_{\mathscr{C}}\frac{df}{f}$ 的两个表达式, 并令其相等, 取极限之后便得到公式(20).

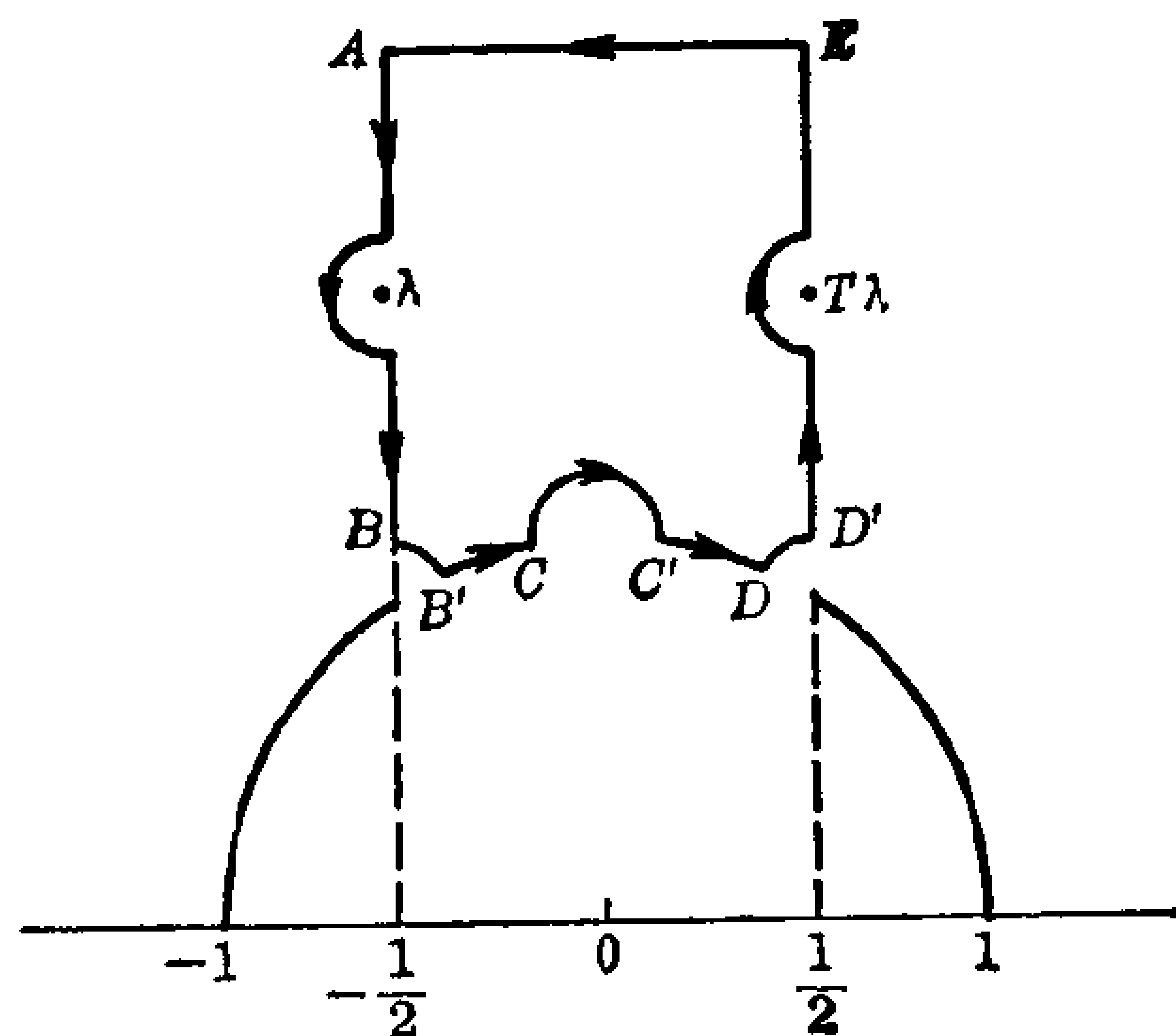


图 3

2) 假如 f 在半直线

$$\left\{z\,\middle|\,\mathrm{Re}(z)=-1/2,\ \mathrm{Im}(z)>\frac{\sqrt{3}}{2}\right\}$$

上有零点或极点 λ, 可以将围道在 λ 和 $T\lambda$ 之邻域内稍加变化(如图3所示, 绕 $T\lambda$ 之圆弧是绕 λ 之圆弧经 T 变换

而得到的)，然后重复上面的证明即可.

如果 f 在 D 的边界上有几个零点或极点，也可以用类似的方法去作.

注 如果在 H/G 的紧致化上定义一个复解析结构，可以避免这个比较复杂的证明（例如见复乘法讨论班，Lecture Notes on Math., n°21, II).

3.2. 模形式代数

如果 k 是整数，我们以 M_k 和 M_k^0 分别表示权 $2k$ 模形式的 $\mathbf{C}$-向量空间和权 $2k$ cusp 型的 $\mathbf{C}$-向量空间，见§2.1定义4. 根据定义，M_k^0 是 M_k 上线性型 $f\mapsto f(\infty)$ 的核. 因此 dim $M_k/M_k^0\leqslant 1$. 此外若 $k\geqslant 2$, Eisenstein 级数 G_k 是 M_k 中元素，使得 $G_k(\infty)\neq 0$（见§2.3命题4)，从而

$$M_k=M_k^0\oplus\mathbf{C}\cdot G_k\quad (k\geqslant 2 \text{ 时}).$$

最后我们记得曾经以 Δ 表示 M_6^0 中元素 $g_2^3-27g_3^2$，其中

$$g_2=60G_2,\qquad g_3=140G_3.$$

定理4 (i) 当 $k<0$ 和 $k=1$ 时，$M_k=0$.

(ii) 当 $k=0, 2, 3, 4, 5$ 时，M_k 是一维向量空间，其基分别为 $1, G_2, G_3, G_4, G_5$. 而 $M_k^0=0$.

(iii) 乘以 Δ 的映射是 M_{k-6} 到 M_k^0 上的同构.

证 设 f 是 M_k 中非零元素. 公式

$$(20)\qquad v_\infty(f)+\frac{1}{2}v_i(f)+\frac{1}{3}v_\rho(f)+\sum_{p\in H/G}{}' v_p(f)=\frac{k}{6}$$

的左边诸项均 $\geqslant 0$，因此 $k\geqslant 0$，而且由于 1/6 不能写成

$$n+n'/2+n''/3,\qquad n,\ n',\ n''\geqslant 0,$$

从而 $k\neq 1$. 这就证明了(i).

现在于公式(20)中取 $f=G_k$, $k=2$. 我们将 2/6 写成

$n+n'/2+n''/3$ 的形式，$n, n', n''\geqslant 0$，这只能是 $n=n'=0$，$n''=1$. 这就表明 $v_\rho(G_2)=1$ 而当 $p\neq\rho(\mathrm{mod}\, G)$ 时 $v_p(G_2)=0$. 同样用于 G_3 即可证明 $v_i(G_3)=1$ 而在其余点 $v_p(G_3)=0$. 这就已经证明了 Δ 在 i 不为 0，从而 Δ 不恒为零. 由于 Δ 的权为 12 而 $v_\infty(\Delta)\geqslant 1$，由公式(20)给出 $v_\infty(\Delta)=1$，并且当 $p\neq\infty$ 时 $v_p(\Delta)=0$. 换句话说，Δ 在 H 上没有零点，而在 ∞ 有一个单零点. 如果 $f\in M_k^0$ 并且令 $g=f/\Delta$，显然 g 的权是 $2k-12$. 而且公式

$$v_p(g)=v_p(f)-v_p(\Delta)=\begin{cases} v_p(f), & \text{如果 } p\neq\infty, \\ v_p(f)-1, & \text{如果 } p=\infty \end{cases}$$

表明对所有 p 均有 $v_p(g)\geqslant 0$，因此 $g\in M_{k-6}$，这就证明了(iii).

最后，如果 $k\leqslant 5$，则 $k-6<0$，由(i)和(iii)可知 $M_k^0=0$. 这就表明 $\dim M_k\leqslant 1$. 由于 $1, G_2, G_3, G_4, G_5$ 分别是 M_0, M_2, M_3, M_4, M_5 中非零元素，我们有 $\dim M_k=1$(对于 $k=0, 2, 3, 4, 5$)，这就证明了(ii).

系 1 我们有

$$\text{(21)}\quad \dim M_k=\begin{cases} \left[\dfrac{k}{6}\right], & \text{如果 } k\equiv 1 (\mathrm{mod}\, 6),\ k\geqslant 0, \\ \left[\dfrac{k}{6}\right]+1, & \text{如果 } k\not\equiv 1 (\mathrm{mod}\, 6),\ k\geqslant 0. \end{cases}$$

(这里 $[x]$ 表示 x 的整数部分，即满足 $n\leqslant x$ 的最大整数 n.)

证 公式(21)对于 $0\leqslant k<6$ 是正确的. 此外，当将 k 改成 $k+6$ 时，表达式增加 1(见(iii))，因此这公式对于每个 $k\geqslant 0$ 均正确.

系 2 单项式集合 $\{G_2^\alpha G_3^\beta \mid 2\alpha+3\beta=k,\ \alpha, \beta\geqslant 0 \text{ 整}\}$ 构成空间 M_k 的一组基.

证 我们首先证明这些单项式生成 M_k. 当 $k\leqslant 3$ 时，这

由(i)和(ii)是显然的. 当 $k\geqslant 4$ 时，我们对 k 归纳. 取非负整数对(γ, δ)使 $2\gamma+3\delta=k$(对每个 $k\geqslant 2$ 这都是可能的). 模形式 $g=G_2^{\gamma}G_3^{\delta}$ 在 ∞ 处不为零. 如果 $f\in M_k$,则存在 $\lambda\in \mathbf{C}$,使 $f-\lambda g$ 为 cusp 型，于是它等于 Δh, $h\in M_{k-6}$, 见(iii). 然后对 h 利用归纳假设即可.

剩下要证明这些单项式是线性无关的. 若不然，函数 G_2^3/G_3^2 将满足一个非平凡的复系数代数方程，从而它必然是常数. 但这是不可能的，因为 G_2 在 ρ 为零，而 G_3 在 ρ 不为零.

注 设 $M=\sum\limits_{k=0}^{\infty} M_k$ 是分次(graded)代数，即是诸 M_k 的直和. 令 $\varepsilon:\mathbf{C}[X, Y]\to M$ 是同态，它将 X 和 Y 分别映成 G_2 和 G_3. 则系 2 可以等价地说成：ε 是同构. 于是可以将 M 等同于多项式代数 $\mathbf{C}[G_2, G_3]$.

3.3. 模不变量

我们令

$$j=1728g_2^3/\Delta. \tag{22}$$

命题 5 (a) 函数 j 是权 0 模函数.

(b) j 在 H 中全纯并且在 ∞ 有单极点.

(c) 转到商中则 j 定义了 H/G 到 $\mathbf{C}$ 上的一个同构.

证 由 g_2^3 和 Δ 的权均为 12 即可证得(a). 由于 Δ 在 H 上不等于 0 而在 ∞ 有单零点，但是 g_2 在 ∞ 不为 0 即可得到(b). 为了证明(c)，我们必须证明如果 $\lambda\in\mathbf{C}$, 则模形式

$$f_\lambda=1728g_2^3-\lambda\Delta$$

有唯一的零点 (mod G). 将公式 (20) 用于 $f=f_\lambda$ 和 $k=6$ 即可证明这一点. 因为 $k/6=1$ 若有形式 $n+n'/2+n''/3$, n, n', $n''\geqslant 0$, 必然

$(n, n', n'') = (1, 0, 0)$, $(0, 2, 0)$或者$(0, 0, 3)$.
这就证明了 f 在 H/G 上只有唯一的零点.

命题 6 设 f 是 H 上亚纯函数, 则下列诸性质彼此等价:

(i) f 是权 0 的模函数;

(ii) f 是权相同的两个模形式之商;

(iii) f 是 j 的有理函数.

证 显然有 (iii)⇒(ii)⇒(i). 现在我们证明 (i)⇒(iii). 设 f 是模函数, 必要时对 f 适当地乘以 j 的一个多项式, 我们可设 f 在 H 上全纯. 因为 Δ 在 ∞ 有零点, 从而有整数 $n \geqslant 0$, 使 $g = \Delta^n f$ 在 ∞ 也全纯. 函数 g 是权 $12n$ 的模形式, 根据定理 4 的系 2, 我们可以将它写成一些 $G_2^\alpha G_3^\beta (2\alpha + 3\beta = 6n)$ 的线性组合. 由于线性, 我们可以设 $g = G_2^\alpha G_3^\beta$, 即 $f = G_2^\alpha G_3^\beta / \Delta^n$. 但是 $2\alpha + 3\beta = 6n$ 表明 $p = \alpha/3$ 和 $q = \beta/2$ 均是整数. 于是

$$f = G_2^{3p} G_3^{2q} / \Delta^{p+q}.$$

从而又将问题归结为证明 G_2^3/Δ 和 G_3^2/Δ 是 j 的有理函数, 而这是显然的.

注 1) 如上所述, 在 H/G 的紧致化 $\widehat{H/G}$ 上可以用自然方式定义一个复解析流形结构. 于是命题 5 即是说 j 定义出 $\widehat{H/G}$ 到 Riemann 球面 $S_2 = \mathbf{C} \cup \{\infty\}$ 之上的同构. 而命题 6 是一个熟知的事实, 即 S_2 上的亚纯函数均为有理函数.

2) 系数 $1728 = 2^6 \cdot 3^3$ 的引进是为了使 j 在 ∞ 处的残数等于 1. 更确切地说, §4 中的级数展开表明:

$$j(z) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n) q^n \quad (z \in H,\ q = e^{2\pi i z}), \tag{23}$$

我们有 $c(1) = 2^2 \cdot 3^3 \cdot 1823 = 196,884;$

$c(2) = 2^{11} \cdot 5 \cdot 2099 = 21,493,760.$

$c(n)$均是整数，并且它们有许多有趣的同余性质[注1]

$$n\equiv 0 \pmod{2^a} \Rightarrow c(n)\equiv 0 \pmod{2^{3a+8}},$$
$$n\equiv 0 \pmod{3^a} \Rightarrow c(n)\equiv 0 \pmod{3^{2a+3}},$$
$$n\equiv 0 \pmod{5^a} \Rightarrow c(n)\equiv 0 \pmod{5^{a+1}},$$
$$n\equiv 0 \pmod{7^a} \Rightarrow c(n)\equiv 0 \pmod{7^a},$$
$$n\equiv 0 \pmod{11^a} \Rightarrow c(n)\equiv 0 \pmod{11^a}.$$

§4. 在∞处的展开

4.1. Bernoulli 数 B_k

B_k 由下面的幂级数展开式定义[注2]:

(24) $$\frac{x}{e^x-1}=1-\frac{x}{2}+\sum_{k=1}^{\infty}(-1)^{k+1}B_k\frac{x^{2k}}{(2k)!}.$$

数值表:

n	1	2	3	4	5	6	7	8	9	10
B_n	$\frac{1}{6}$	$\frac{1}{30}$	$\frac{1}{42}$	$\frac{1}{30}$	$\frac{5}{66}$	$\frac{691}{2730}$	$\frac{7}{6}$	$\frac{3617}{510}$	$\frac{43867}{798}$	$\frac{283\times 617}{330}$

n	11	12	13	14
B_n	$\frac{11\times 131\times 593}{138}$	$\frac{103\times 2294797}{2730}$	$\frac{13\times 657931}{6}$	$\frac{7\times 9349\times 362903}{870}$

[注1] 关于这方面可见 A. O. L. Atkin 和 J. N. L'Brien, Trans. Amer. Math. Soc., 126, 1967, 以及 Atkin 在"Computers in mathematical research" (North Holland, 1968) 中的文章。

[注2] 在一些文献上还可以发现将 Bernoulli 数 b_k 用下式定义:

$$\frac{x}{e^x-1}=\sum_{k=0}^{\infty}b_k x^k/k!,$$

于是 $b_0=1$, $b_1=-1/2$, $b_{2k+1}=0$ ($k>1$ 时), 而 $b_{2k}=(-1)^{k-1}B_k$. 在研究同余性质的时候和 Leopoldt 将 Bernoulli 数作推广的时候, 用符号 b 更合适些.

B_k 给出 Riemann zeta 函数在正偶整数处的值（和在负奇整数处的值）：

命题 7 如果 $k\geqslant 1$ 是整数，则

$$\zeta(2k)=\frac{2^{2k-1}}{(2k)!}B_k\pi^{2k}. \tag{25}$$

证 在 B_k 的定义公式中取 $x=2iz$ 即得到恒等式

$$z\operatorname{ctg} z=1-\sum_{k=1}^{\infty}B_k\frac{2^{2k}z^{2k}}{(2k)!}. \tag{26}$$

另一方面，将

$$\sin z=z\prod_{n=1}^{\infty}\left(1-\frac{z^2}{n^2\pi^2}\right) \tag{27}$$

取对数微商，得到

$$z\operatorname{ctg} z=1+2\sum_{n=1}^{\infty}\frac{z^2}{z^2-n^2\pi^2}=1-2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{z^{2k}}{n^{2k}\pi^{2k}}. \tag{28}$$

比较公式(26)和(28)，即得(25)式.

【例】

$$\zeta(2)=\frac{\pi^2}{2\times 3},\quad \zeta(4)=\frac{\pi^4}{2\times 3^2\times 5},\quad \zeta(6)=\frac{\pi^6}{3^3\times 5\times 7},$$

$$\zeta(8)=\frac{\pi^8}{2\times 3^3\times 5^2\times 7},\quad \zeta(10)=\frac{\pi^{10}}{3^5\times 5\times 7\times 11},$$

$$\zeta(12)=\frac{691\cdot\pi^{12}}{3^6\times 5^3\times 7^2\times 11\times 13},$$

$$\zeta(14)=\frac{2\pi^{14}}{3^6\times 5^2\times 7\times 11\times 13}.$$

4.2. 函数 G_k 的级数展开

现在给出 Eisenstein 级数 $G_k(z)$ 关于 $q=e^{2\pi iz}$ 的 Taylor 展开式. 我们先从熟知的公式开始:

$$(29)\qquad \pi\operatorname{ctg}\pi z=\frac{1}{z}+\sum_{m=1}^{\infty}\left(\frac{1}{z+m}+\frac{1}{z-m}\right).$$

另一方面我们有

$$(30)\qquad \pi\operatorname{ctg}\pi z=\pi\frac{\cos\pi z}{\sin\pi z}=i\pi\frac{q+1}{q-1}$$

$$=i\pi-\frac{2\pi i}{1-q}=\pi i-2\pi i\sum_{n=0}^{\infty}q^n.$$

比较一下即得

$$(31)\qquad \frac{1}{z}+\sum_{m=1}^{\infty}\left(\frac{1}{z+m}+\frac{1}{z-m}\right)=\pi i-2\pi i\sum_{n=0}^{\infty}q^n.$$

将(31)式逐次微商，就得到以下的公式(它在 $k\geqslant 2$ 时是对的)：

$$(32)\qquad \sum_{m\in\mathbf{Z}}\frac{1}{(m+z)^k}=\frac{1}{(k-1)!}(-2\pi i)^k\sum_{n=1}^{\infty}n^{k-1}q^n.$$

现在以 $\sigma_k(n)$ 表示 n 的全部正因子的 k 次幂之和 $\sum_{d|n}d^k$.

命题 8 对于每个整数 $k\geqslant 2$, 我们有

$$(33)\qquad G_k(z)=2\zeta(2k)+2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n.$$

证 展开:

$$G_k(z)=\sum_{(m,n)\neq(0,0)}\frac{1}{(nz+m)^{2k}}$$

$$=2\zeta(2k)+2\sum_{n=1}^{\infty}\sum_{m\in\mathbf{Z}}\frac{1}{(nz+m)^{2k}}.$$

应用以 nz 代替 z 的(32)式，得到

$$G_k(z)=2\zeta(2k)+\frac{2(-2\pi i)^{2k}}{(2k-1)!}\sum_{d=1}^{\infty}\sum_{a=1}^{\infty}d^{2k-1}q^{ad}$$

$$=2\zeta(2k)+\frac{2(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n.$$

系 $G_k(z)=2\zeta(2k)E_k(z)$, 其中

(34) $$E_k(z)=1+\gamma_k\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n.$$

而

(35) $$\gamma_k=(-1)^k\frac{4k}{B_k}.$$

证 由于 $E_k(z)=G_k(z)/2\zeta(2k)$，显然有(34)式，其中系数 γ_k 用命题 7 计算：

$$\gamma_k=\frac{(2\pi i)^{2k}}{(2k-1)!}\frac{1}{\zeta(2k)}=\frac{(2\pi)^{2k}(-1)^k}{(2k-1)!}\cdot\frac{(2k)!}{2^{2k-1}B_k\pi^{2k}}$$
$$=(-1)^k\frac{4k}{B_k}.$$

【例】

$$E_2=1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n,\qquad g_2=(2\pi)^4\frac{1}{2^2\times 3}E_2.$$

$$E_3=1-504\sum_{n=1}^{\infty}\sigma_5(n)q^n,\qquad g_3=(2\pi)^6\frac{1}{2^3\times 3^3}E_3.$$

$$E_4=1+480\sum_{n=1}^{\infty}\sigma_7(n)q^n.$$

$$E_5=1-264\sum_{n=1}^{\infty}\sigma_9(n)q^n.$$

$$E_6=1+\frac{65520}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n$$
$$(65520=2^4\times 3^2\times 5\times 7\times 13).$$

$$E_7=1-24\sum_{n=1}^{\infty}\sigma_{13}(n)q^n.$$

注 我们在§3.2中已经知道，权 8 和权 10 的模形式空间的维数都是 1，于是

(36) $$E_2^2=E_4,\quad E_2E_3=E_5.$$

这等价于恒等式

$$\sigma_7(n)=\sigma_3(n)+120\sum_{m=1}^{n-1}\sigma_3(m)\sigma_3(n-m).$$

$$11\sigma_9(n)=21\sigma_5(n)-10\sigma_3(n)+5040\sum_{m=1}^{n-1}\sigma_3(m)\sigma_5(n-m).$$

更一般地，每个 E_k 可以表示成 E_2 和 E_3 的多项式.

4.3. 模形式系数的估计

令

$$f(z)=\sum_{n=0}^{\infty}a_nq^n \quad (q=e^{2\pi iz}) \tag{37}$$

是权 $2k(k\geqslant 2)$ 的模形式. 我们对于数 a_n 的增长情况感兴趣.

命题 9 如果 $f=G_k$, 则 a_n 的阶为 n^{2k-1}. 更确切地说，存在两个常数 A, $B>0$, 使得

$$An^{2k-1}\leqslant|a_n|\leqslant Bn^{2k-1}. \tag{38}$$

证 命题 8 证明了存在正常数 A, 使得

$$a_n=(-1)^kA\sigma_{2k-1}(n),$$

于是 $|a_n|=A\sigma_{2k-1}(n)\geqslant An^{2k-1}$. 另一方面,

$$\frac{|a_n|}{n^{2k-1}}=A\sum_{d|n}\frac{1}{d^{2k-1}}\leqslant A\sum_{d=1}^{\infty}\frac{1}{d^{2k-1}}=A\zeta(2k-1)<+\infty.$$

定理 5(Hecke) 如果 f 是权 $2k$ 的 cusp 型，则

$$a_n=O(n^k). \tag{39}$$

(换句话说，当 $n\to\infty$ 时商 $\dfrac{|a_n|}{n^k}$ 保持为有界.)

证 因为 f 是 cusp 型，我们有 $a_0=0$, 从 f 的展开式(37)中可以析出一个因子 q. 于是，当 $q\to 0$ 时,

$$|f(z)|=O(q)=O(e^{-2\pi y}), \tag{40}$$

其中

$$y=\mathrm{Im}(z).$$

令 $\phi(z)=|f(z)|y^k$. 公式(1)和(2)表明 ϕ 在模群 G 之下

不变. 此外，ϕ 在基本区域 D 上连续，而公式(40)表明当 $y\to\infty$ 时 ϕ 趋于 0. 这就推得 ϕ 是有界的，即存在常数 M 使得

$$(41)\qquad |f(z)|\leqslant My^{-k}\quad (z\in H).$$

固定 y 而让 x 在 0 到 1 之间变化. 点 $q=e^{2\pi i(x+iy)}$ 跑过中心在 0 的圆周 C_y. 由残数公式，

$$a_n=\frac{1}{2\pi i}\int_{C_y}f(z)q^{-n-1}dq=\int_0^1 f(x+iy)q^{-n}dx.$$

(还可以从周期函数的 Fourier 系数推出这个公式.)

利用公式(41)，可以由此得到

$$|a_n|\leqslant My^{-k}e^{2\pi ny}.$$

这个不等式对于所有的 $y>0$ 都是对的，取 $y=\dfrac{1}{n}$，就给出

$$|a_n|\leqslant e^{2\pi}Mn^k,$$

由此证明了定理.

系 如果 f 不是 cusp 型，则 a_n 的阶是 n^{2k-1}.

证 我们将 f 写成形式 λG_k+h, $\lambda\neq 0$, h 为 cusp 型. 然后利用命题 9 和定理 5 即可，因为 n^k 与 n^{2k-1} 相比前者是可以"忽略"掉的.

注 定理 5 的指数 k 可以改进. 我们有

$$a_n=O(n^{k-\frac{1}{4}+\varepsilon})\quad (对任意\ \varepsilon>0).$$

(见 A. Selberg, Proc. Symp. Pure Maths. VIII, Amer. Math. Soc., 1965.) 甚至猜想 k 可代之以 $k-\dfrac{1}{2}+\varepsilon$ (对任意 $\varepsilon>0$)，或者等价地:

$$a_n=O(n^{k-1/2}\sigma_0(n)),$$

其中 $\sigma_0(n)$ 是 n 的因子个数. 我们在 § 5.6 中还要回到这个问题上来.

4.4. Δ 的展开式

注意到

$$
\Delta = g_2^3 - 27g_3^2 = (2\pi)^{12}2^{-6}3^{-3}(E_2^3 - E_3^2)
\tag{42}
$$

$$
= (2\pi)^{12}(q - 24q^2 + 252q^3 - 1472q^4 + \cdots).
$$

定理 6 (Jacobi)

$$
\Delta = (2\pi)^{12}q\prod_{n=1}^{\infty}(1-q^n)^{24}.
$$

[这个公式用椭圆函数的方法证明最为自然. 由于这个方法要使我们走太远的路, 所以在下面简述另外一个证明, 这个证明是初等的, 但却是有些"人为"的. 详见 A. Hurwitz, Math. Werke, Bd. 1, pp. 578~595.]

证 令

$$
F(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}.
\tag{43}
$$

为了证明 F 和 Δ 是成比例的, 只需证明 F 是权 12 的模形式. 事实上, F 的展开式的常数项为 0, 从而 F 是 cusp 型. 此外我们知道(定理 4), 权 12的 cusp 型空间 M_6^0 的维数是 1. 由 § 2.1 的命题 1, 我们只需证明

$$
F\left(-\frac{1}{z}\right) = z^{12}F(z).
\tag{44}
$$

为此, 我们使用双重级数

$$
G_1(z) = \sum_n\sum_m{}' \frac{1}{(m+nz)^2}, \qquad G(z) = \sum_m\sum_n{}' \frac{1}{(m+nz)^2}.
$$

$$
H_1(z) = \sum_n\sum_m{}' \frac{1}{(m-1+nz)(m+nz)},
$$

$$
H(z) = \sum_m\sum_n{}' \frac{1}{(m-1+nz)(m+nz)}.
$$

其中对于 G 和 G_1，符号 $\sum'$ 表示 (m, n) 过一切

$$(m, n) \neq (0, 0), \qquad m, n \in \mathbf{Z};$$

而对于 H_1 和 H，$\sum'$ 表示 (m, n) 过一切 $(m, n) \neq (0, 0)$ 和 $(1, 0)$.（注意求和次序！）

级数 H_1 和 H 容易明显计算，因为有公式

$$\frac{1}{(m-1+nz)(m+nz)} = \frac{1}{m-1+nz} - \frac{1}{m+nz}.$$

我们发现它们均收敛，而且

$$H_1 = 2, \qquad H = 2 - 2\pi i/z.$$

进而，通项为

$$\frac{1}{(m-1+nz)(m+nz)} - \frac{1}{(m+nz)^2}$$

$$= \frac{1}{(m+nz)^2(m-1+nz)}$$

的双重级数是可以绝对求和的．这表明 $G_1 - H_1 = G - H$. 从而级数 G 和 G_1 收敛（对于所示的求和次序），并且

$$G_1(z) - G(z) = H_1(z) - H(z) = \frac{2\pi i}{z}.$$

显然 $G_1(-1/z) = z^2 G(z)$，于是

$$G_1(-1/z) = z^2 G_1(z) - 2\pi i z. \tag{45}$$

另一方面，类似于命题 8 的一个计算给出

$$G_1(z) = \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n) q^n. \tag{46}$$

现在回到由(43)定义的函数 F．它的对数微商是

$$\frac{dF}{F} = \frac{dq}{q}\left(1 - 24 \sum_{n, m=1}^{\infty} n q^{nm}\right) \tag{47}$$

$$= \frac{dq}{q}\left(1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n\right).$$

与(46)比较，我们得到

$$(48)\qquad \frac{dF}{F}=\frac{6i}{\pi}G_1(z)dz.$$

比较(45)和(48)两式，我们有

$$(49)\qquad \frac{dF(-1/z)}{F(-1/z)}=\frac{6i}{\pi}G_1(-1/z)\frac{dz}{z^2}$$

$$=\frac{6i}{\pi}\frac{dz}{z^2}(z^2G_1(z)-2\pi iz)$$

$$=\frac{dF(z)}{dz}+12\frac{dz}{z}.$$

于是两个函数 $F(-1/z)$ 和 $z^{12}F(z)$ 有同样的对数微商. 从而存在一个常数 k, 使得

$$F(-1/z)=kz^{12}F(z)\quad (对于每个\ z\in H).$$

对于 $z=i$, 我们有 $z^{12}=1$, $-1/z=z$, 而 $F(z)\neq 0$. 这证明 $k=1$, 从而证明了(44)式. 证毕.

注 在 C. L. Siegel, Gesamm. Abh., III, n°62 中可以找到恒等式(44)的另一个"初等"证明. 还见«复乘法讨论班», III, § 6.

4.5. Ramanujan 函数

以 $\tau(n)$ 表示 cusp 型 $F(z)=(2\pi)^{-12}\Delta(z)$ 的第 n 个系数. 于是有

$$(50)\qquad \sum_{n=1}^{\infty}\tau(n)q^n=q\prod_{n=1}^{\infty}(1-q^n)^{24}.$$

函数 $n\mapsto\tau(n)$ 叫作 Ramanujan 函数.

数值表[注]

[注] 此表取自 D. H. Lehmer, Ramanujan's function $\tau(n)$, Duke Math. J., 10, 1943, 该文给出 $n\leqslant 300$ 的全部 $\tau(n)$ 值.

n	1	2	3	4	5	6	7
$\tau(n)$	1	-24	252	-1472	4830	-6048	-16744

n	8	9	10	11	12
$\tau(n)$	84480	-113643	-115920	534612	-370944

$\tau(n)$的性质:

(51) $$\tau(n)=O(n^6).$$

这是因为 Δ 的权为 12, 见 § 4.3 定理 5.

(52) $$\tau(nm)=\tau(n)\tau(m) \quad (\text{如果}(n,\ m)=1).$$

(53) $$\tau(p^{n+1})=\tau(p)\tau(p^n)-p^{11}\tau(p^{n-1}),$$

$$p\text{ 为素数, } n>1 \quad (\text{见下面 § 5.5}).$$

恒等式 (52) 和 (53) 是由 Ramanujan 猜想而首先由 Mordell 证明的. 我们可以将它重述成: Dirichlet 级数

$$L_\tau(s)=\sum_{n=1}^{\infty}\tau(n)/n^s$$

有下面的 Euler 展开式:

(54) $$L_\tau(s)=\prod_{p\in P}\frac{1}{1-\tau(p)p^{-s}+p^{11-2s}} \quad (\text{见 § 5.4}).$$

根据 Hecke 定理(见 § 5.4), 函数 L_τ 可以延拓成复平面上的整函数, 并且函数

$$(2\pi)^{-s}\Gamma(s)L_\tau(s)$$

在 $s\mapsto 12-s$ 之下是不变的.

$\tau(n)$对于 mod 2^{12}, 3^6, 5^3, 7, 23, 691 有各种有趣的同余关系. 我们摘录一些特殊情形(不加证明):

(55) $$\tau(n) \equiv n^2\sigma_7(n) \pmod{3^3},$$

(56) $$\tau(n) \equiv n\sigma_3(n) \pmod{7},$$

(57) $$\tau(n) \equiv \sigma_{11}(n) \pmod{691}.$$

关于另一些例子和它用"l-adic 表示"的解释，可见 Delange-Pisot-Poitou 讨论班 1967/1968, 第 14 讲; Bourbaki 讨论班 1968/1969 第 355 讲和 1971/1972 第 416 讲.

最后我们谈两个未解决的问题:

a) (Ramanujan 猜想见 § 5.6) 是否对于每个素数 p 均有 $|\tau(p)| < 2p^{11/2}$?(*)

b) (Lehmer)是否对每个 n 均有 $\tau(n) \neq 0$?

§ 5. Hecke 算子

5.1. $T(n)$ 的定义

对应 设 E 是一个集合，令 X_E 是由 E 生成的自由 Abel 群. E 上的一个(具有整系数的)对应(correspondence)是 X_E 到自身之中的同态 T. 为了给出 T，我们只需给出它在 E 之全部元素 x 的取值:

(58) $$T(x) = \sum_{y \in E} n_y(x) y, \quad n_y(x) \in \mathbf{Z},$$

其中对几乎所有的 y, $n_y(x) = 0$.

设 F 是 E 上的数值函数. 它可以 $\mathbf{Z}$- 线性地扩充成 X_E 上的函数，仍记为 F. F 经过 T 的变换是函数 $F \circ T$ 在 E 上的限制，这个函数记成 TF. 采用(58)的记号我们有

(59) $$TF(x) = F(T(x)) = \sum_{y \in E} n_y(x) F(y).$$

算子 $T(n)$ 设 $\mathscr{R}$ 是 $\mathbf{C}$ 上的全部格所构成的集合(见

(*) 这一猜想已为 P. Deligne 所证明，见: P. Deligne, La conjecture de Weil, I, Publ. I. H. E. S. 43 (1974), 273~307.——译者注

§ 2.2). 令 $n \geqslant 1$ 为整数. 我们以 $T(n)$ 表示 $\mathscr{R}$ 上的一个对应, 它把一个格变换成它的所有指数为 n 的子格之和(这是 $X_{\mathscr{R}}$ 中元素). 于是我们有

(60) $$T(n)\Gamma = \sum_{(\Gamma:\Gamma')=n} \Gamma' \quad (\text{对于 } \Gamma \in \mathscr{R}).$$

右边的和式是有限和. 事实上, 所有的格 Γ' 均包含 $n\Gamma$, 而其个数也等于 $\Gamma/n\Gamma = (\mathbf{Z}/n\mathbf{Z})^2$ 的 n 阶子群的个数. 如果 n 为素数, 易知这个数等于 $n+1$ (即 n 元域上射影直线中的点数).

我们还使用一个相似算子 $R_\lambda (\lambda \in \mathbf{C}^*)$, 它定义为

(61) $$R_\lambda \Gamma = \lambda \Gamma \quad (\Gamma \in \mathscr{R}).$$

一些公式　对应 $T(n)$ 和 R_λ 都是 Abel 群 $X_{\mathscr{R}}$ 的自同态, 因此它们的合成是有意义的.

命题 10　对应 $T(n)$ 和 R_λ 有如下的恒等式:

(62) $$R_\lambda R_\mu = R_{\lambda\mu} \quad (\lambda, \mu \in \mathbf{C}^*),$$

(63) $$R_\lambda T(n) = T(n) R_\lambda \quad (n \geqslant 1, \lambda \in \mathbf{C}^*),$$

(64) $$T(m)T(n) = T(mn) \quad (\text{如果}(m, n) = 1),$$

(65) $$T(p^n)T(p) = T(p^{n+1}) + pT(p^{n-1})R_p \quad (p \text{ 为素数}, n \geqslant 1).$$

证　公式(62)和(63)是显然的.

公式(64)等价于下面的论断: 设 $(m, n) = 1$, $m, n \geqslant 1$, 令 Γ'' 是格 Γ 的指数为 mn 的子格, 则存在 Γ 的唯一的一个子格 Γ', 使得 $\Gamma' \supset \Gamma''$, 并且 $(\Gamma:\Gamma') = n$, $(\Gamma':\Gamma'') = m$. 这个论断是由于群 Γ/Γ'' 的阶为 mn, 它可唯一地分解成一个 m 阶群和一个 n 阶群的直和(Bezout 定理).

为了证明 (65), 令 Γ 是一个格, 则 $T(p^n)T(p)\Gamma$, $T(p^{n+1})\Gamma$ 和 $T(p^{n-1})R_p\Gamma$ 均是 Γ 中指数为 p^{n+1} 的一些格的

线性组合（注意 $(\Gamma:R_p\Gamma)=p^2$）．以 Γ'' 表示这样的一个格，并设它在上面的三个线性组合公式中的系数分别为 a，b 和 c．我们要证明 $a=b+pc$，即要证明 $a=1+pc$，因为 b 显然等于 1．

我们有两种情形：

i) Γ'' 不包含在 $p\Gamma$ 中．则 $c=0$，而 a 为满足条件 $\Gamma''\subset\Gamma'\subset\Gamma$，$(\Gamma:\Gamma')=p$ 的格 Γ' 的个数．这样一个格包含 $p\Gamma$．在 $\Gamma/p\Gamma$ 中，Γ' 的象的指数为 p，它包含有 Γ'' 的象，而后者的阶数为 p（从而指数也是 p，因为 $\Gamma/p\Gamma$ 的阶数为 p^2）．于是只有一个 Γ'．这给出 $a=1$，即公式 $a=1+pc$ 是正确的．

ii) $L''\subset p\Gamma$．我们有 $c=1$．每个在 Γ 中指数为 p 的格 Γ' 均包含 $p\Gamma$，从而也包含 L''．这给出 $a=p+1$，即公式 $a=1+pc$ 也正确．

系 1 $T(p^n)\,(n>1)$ 是 $T(p)$ 和 R_p 的多项式．

证 对 n 归纳，由公式(65)即可推出．

系 2 由 R_λ 和 $\{T(p)\,|\,p$ 为素数$\}$ 生成的代数是交换代数．它包含全部 $T(n)$．

证 由命题 10 和系 1 即可推出．

$T(n)$ 在权 $2k$ 的函数上的作用

设 F 是权 $2k$ 的 $\mathscr{R}$ 上函数（见 § 2.2）．由定义

(66) $$R_\lambda F=\lambda^{-2k}F \quad (\text{对一切 } \lambda\in\mathbf{C}^*).$$

设 n 为自然数．公式(63)表明

$$R_\lambda(T(n)F)=T(n)(R_\lambda F)=\lambda^{-2k}T(n)F,$$

换句话说，$T(n)F$ 的权也是 $2k$．公式(64)和(65)给出：

(67) $$T(m)T(n)F=T(mn)F \quad (\text{如果 } (m,\,n)=1).$$

$$(68)\qquad T(p)T(p^n)F = T(p^{n+1})F + p^{1-2k}T(p^{n-1})F$$
$$(p\text{ 素数},\ n\geqslant 1).$$

5.2. 一个关于矩阵的引理

设 Γ 是基为 $\{\omega_1, \omega_2\}$ 的格，n 为自然数. 下面的引理给出 Γ 的全部指数为 n 的子格.

引理 2 设

$$S_n = \left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a、b、d \text{ 为整数},\ ad = n,\ a \geqslant 1,\ 0 \leqslant b < d\right\}.$$

如果 $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_n$，以 Γ_σ 表示基为

$$\omega_1' = a\omega_1 + b\omega_2, \qquad \omega_1' = d\omega_2$$

的 Γ 之子格. 则映射 $\sigma \mapsto \Gamma_\sigma$ 是从 S_n 到 $\Gamma(n)$ 之上的一一映射. 其中 $\Gamma(n)$ 是 Γ 中指数为 n 的子格全体所构成的集合.

证 因为 $\det(\sigma) = n$，从而 $\Gamma_\sigma \in \Gamma(n)$. 反之，令 $\Gamma' \in \Gamma(n)$，我们取

$$Y_1 = \Gamma/(\Gamma' + \mathbf{Z}\omega_2), \qquad Y_2 = \mathbf{Z}\omega_2/(\Gamma' \cap \mathbf{Z}\omega_2).$$

它们分别是由 ω_1 和 ω_2 的象所生成的循环群. 设它们的阶数分别为 a 和 d. 由于有正合列

$$0 \to Y_2 \to \Gamma/\Gamma' \to Y_1 \to 0,$$

从而 $ad = n$. 如果 $\omega_2' = d\omega_2$，则 $\omega_2' \in \Gamma'$. 另一方面，存在 $\omega_1' \in \Gamma'$，使得

$$\omega_1' \equiv a\omega_1 \pmod{\mathbf{Z}\omega_2}.$$

显然 ω_1' 和 ω_2' 形成 Γ' 的一组基. 此外，我们可以将 ω_1' 写成形式

$$\omega_1' = a\omega_1 + b\omega_2 \quad (b \in \mathbf{Z}),$$

其中 b 是 $\bmod d$ 唯一决定的. 如果对 b 加上条件 $0 \leqslant b < d$,

这就唯一决定了 b，从而唯一决定了 ω_1'。于是我们对于每个 $\Gamma'\in\Gamma(n)$ 结合一个矩阵 $\sigma(\Gamma')\in S_n$。容易检验映射 $\sigma\mapsto\Gamma_\sigma$ 和 $\Gamma'\mapsto\sigma(\Gamma')$ 彼此互逆，这就证明了引理。

【例】 如果 p 是素数，S_p 中的元素是矩阵 $\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}$ 和 p 个矩阵 $\begin{pmatrix}1 & b\\ 0 & p\end{pmatrix}$ $(0\leqslant b<p)$。

5.3. $T(n)$ 在模函数上的作用

设 k 为整数，f 是权 $2k$ 的弱模函数，见 §2.1. 我们在 §2.2 中已经看到，f 对应于 $\mathscr{R}$ 上一个权 $2k$ 的函数 F，使得

$$F(\Gamma(\omega_1,\ \omega_2))=\omega_2^{-2k}f(\omega_1/\omega_2). \tag{69}$$

我们定义 $T(n)f$ 为与 $\mathscr{R}$ 上函数 $n^{2k-1}T(n)F$ 相结合的 H 上函数(注意数值系数 n^{2k-1}，它使下面的公式中"没有分母")。因此由定义，

$$T(n)f(z)=n^{2k-1}T(n)F(\Gamma(z,\ 1)). \tag{70}$$

或者由引理 2，

$$T(n)f(z)=n^{2k-1}\sum_{\substack{a\geqslant 1,\,ad=n\\ 0\leqslant b<d}} d^{-2k}f\left(\frac{az+b}{d}\right). \tag{71}$$

命题 11 函数 $T(n)f$ 是权 $2k$ 的弱模函数。如果 f 在 H 上全纯，则 $T(n)f$ 也在 H 上全纯。并且有

$$T(m)T(n)f=T(mn)f\quad(\text{如果}(m,\ n)=1). \tag{72}$$

$$T(p)T(p^n)f=T(p^{n+1})f+p^{2k-1}T(p^{n-1})f\quad(p\ \text{素数},\ n\geqslant 1). \tag{73}$$

证 公式(71)表明 $T(n)f$ 在 H 上是亚纯的，从而为弱模函数。此外，如果 f 是全纯的，则 $T(n)f$ 也是全纯的。考虑到 $T(n)f$ 的定义中有数值系数 n^{2k-1}，便知公式(72)和(73)可以从公式(67)和(68)推出。

在 ∞ 处的性状. 设 f 是模函数, 即它在 ∞ 处亚纯. 令

(74) $$f(z)=\sum_{m\in\mathbf{Z}}c(m)q^m$$

是它关于 $q=e^{2\pi iz}$ 的 Laurent 展开式.

命题 12 函数 $T(n)f$ 是模函数. 我们有

(75) $$T(n)f(z)=\sum_{m\in\mathbf{Z}}\gamma(m)q^m,$$

其中

(76) $$\gamma(m)=\sum_{\substack{a\mid(n,m)\\ a\geqslant 1}}a^{2k-1}c\left(\frac{mn}{a^2}\right).$$

证 按照定义我们有

$$T(n)f(z)=n^{2k-1}\sum_{\substack{ad=n,a\geqslant 1\\ 0\leqslant b<d}}d^{-2k}\sum_{m\in\mathbf{Z}}c(m)e^{2\pi im(az+b)/d}.$$

现在 $$\sum_{0\leqslant b<d}e^{2\pi ibm/d}=\begin{cases}d, & \text{如果 } d\mid m,\\ 0, & \text{否则},\end{cases}$$

因此令 $m/d=m'$, 便有

$$T(n)f(z)=n^{2k-1}\sum_{\substack{ad=n\\ a\geqslant 1,m'\in\mathbf{Z}}}d^{-2k+1}c(m'd)q^{am'}.$$

将 q 的同幂次项收集在一起, 便给出

$$T(n)f(z)=\sum_{\mu\in\mathbf{Z}}q^\mu\sum_{\substack{a\mid(n,\mu)\\ a\geqslant 1,ad=n}}\left(\frac{n}{d}\right)^{2k-1}c\left(\frac{\mu d}{a}\right).$$

因为 f 在 ∞ 处亚纯, 从而存在整数 $N\geqslant 0$, 使得当 $m\leqslant -N$ 时 $c(m)=0$. 因此对于 $\mu\leqslant -nN$, 则 $c\left(\frac{\mu d}{a}\right)=0$, 这证明 $T(n)f$ 在 ∞ 处也亚纯. 因为它是弱模函数, 从而它是模函数. 从上面的计算即可给出公式(76).

系 1 $\gamma(0)=\sigma_{2k-1}(n)c(0)$, $\gamma(1)=c(n)$.

系 2 如果 $n=p$ 是素数, 则

$$\gamma(m)=\begin{cases} c(pm), & \text{如果 } m\not\equiv 0 \pmod p,\\ c(pm)+p^{2k-1}c\left(\dfrac{m}{p}\right), & \text{如果 } m\equiv 0 \pmod p. \end{cases}$$

系 3 如果 f 为模形式或者 cusp 型，则 $T(n)f$ 亦然.

这些系显然成立.

于是，$T(n)$ 作用在 § 3.2 的空间 M_k 和 M_k^0 上. 正如我们在上面所看到的，这些算子彼此可交换，并且满足以下的恒等式：

(72) $$T(m)T(n)=T(mn)\quad (\text{如果}(m,\ n)=1).$$

(73) $$T(p)T(p^n)=T(p^{n+1})+p^{2k-1}T(p^{n-1})$$

$$(p\ \text{素数},\ n\geqslant 1).$$

5.4. $T(n)$ 的本征函数

设 $f(z)=\sum\limits_{n=0}^{\infty}c(n)q^n$ 是权 $2k(k>0)$ 的不恒等于零的模形式. 我们假定 f 是所有 $T(n)$ 的本征函数，即存在复数 $\lambda(n)$，使得

(77) $$T(n)f=\lambda(n)f\quad (\text{对于每个 } n\geqslant 1).$$

定理 7 a) f 中 q 的系数 $c(1)\neq 0$.

b) 如果 f 由条件 $c(1)=1$ 标准化，则

(78) $$c(n)=\lambda(n)\quad (\text{对每个 } n\geqslant 1).$$

证 命题 12 的系 1 表明 $T(n)f$ 中 q 的系数是 $c(n)$. 另一方面由 (77) 它也是 $\lambda(n)c(1)$. 于是 $c(n)=\lambda(n)c(1)$. 如果 $c(1)=0$，则所有 $c(n)\,(n>0)$ 均为零，从而 f 为常数，这是不可能的. 于是证明了 a) 和 b).

系 1 两个权 $2k(k>0)$ 的模形式如果均是所有 $T(n)$ 的本征函数，并且有同样的一些 $\lambda(n)$，而且均是标准化了的，那么它们必然相等.

证 将 a) 用于这两个函数之差即可.

系 2 在定理 7, b) 的假设下,

(79) $$c(m)c(n)=c(mn) \quad (\text{如果}(m,n)=1).$$

(80) $$c(p)c(p^n)=c(p^{n+1})+p^{2k-1}c(p^{n-1}).$$

证 事实上, 本征值 $\lambda(n)=c(n)$ 满足与 $T(n)$ 的(72) 和 (73) 相同的恒等式.

公式(79)和(80)可以如下方式解析地加以改变: 令

(81) $$\Phi_f(s)=\sum_{n=1}^{\infty}c(n)/n^s$$

是由 $c(n)$ 定义的 Dirichlet 级数. 根据定理 5 的系, 这个级数对于 $\mathrm{Re}(s)>2k$ 绝对收敛.

系 3 我们有

(82) $$\Phi_f(s)=\prod_{p\in P}\frac{1}{1-c(p)p^{-s}+p^{2k-1-2s}}.$$

证 由(79)式可知函数 $n\mapsto c(n)$ 是积性的. 因此由第七章 § 3.1 引理 4 可知 $\Phi_f(s)$ 是级数 $\sum_{n=0}^{\infty}c(p^n)p^{-ns}$ 之积. 令 $p^{-s}=T$, 我们归结为要证明恒等式

(83) $$\sum_{n=0}^{\infty}c(p^n)T^n=\frac{1}{\Phi_{f,p}(T)},$$

其中 $\Phi_{f,p}(T)=1-c(p)T+p^{2k-1}T^2$. 作级数

$$\psi(T)=\left(\sum_{n=0}^{\infty}c(p^n)T^n\right)(1-c(p)T+p^{2k-1}T^2).$$

ψ 中 T 的系数是 $c(p)-c(p)=0$. 而当 $n\geqslant1$ 时, T^{n+1} 的系数根据(80)是

$$c(p^{n+1})-c(p)c(p^n)+p^{2k-1}c(p^{n-1})=0.$$

因此级数 ψ 只有常数项 $c(1)=1$, 这就证明了(83)式.

注 1) 反过来, 公式(81)和(82)推出公式(79)和(80).

2) Hecke 证明了 Φ_f 可以解析延拓成整个复平面上的亚纯函数(如果 f 是 cusp 型，它甚至可以解析延拓成复平面上的全纯函数)，并且函数

(84) $$X_f(s)=(2\pi)^{-s}\Gamma(s)\Phi_f(s)$$

满足函数方程

(85) $$X_f(s)=(-1)^k X_f(2k-s).$$

证明是使用 Mellin 变换公式

$$X_f(s)=\int_0^\infty (f(iy)-f(\infty))y^s\frac{dy}{y},$$

以及恒等式 $f(-1/z)=z^{2k}f(z)$. Hecke 还证明了其逆：一个 Dirichlet 级数 Φ 如果满足这种类型的函数方程并且加上某些正规性和增长速度的一些假设，则 Φ 必然是从一个权 $2k$ 的模形式 f 所得到的. 而且 f 是 $T(n)$ 的标准化本征函数的充要条件是 Φ 为(82)形式的 Euler 乘积. 详见 E. Hecke 的数学著作集 n°33 和 A. Weil, Math. Annalen, 168(1967).

5.5. 一些例子

a) Eisenstein 级数. 设 $k\geqslant 2$ 为整数.

命题 13 Eisenstein 级数 G_k 是所有 $T(n)$ 的本征函数. 对应的本征值是 $\sigma_{2k-1}(n)$，而标准化本征函数是

(86) $$(-1)^k\frac{B_k}{4k}E_k=(-1)^k\frac{B_k}{4k}+\sum_{n=1}^\infty\sigma_{2k-1}(n)q^n.$$

对应的 Dirichlet 级数是 $\zeta(s)\zeta(s-2k+1)$.

证　我们首先证明 G_k 是 $T(n)$ 的本征函数. 这只要对 $T(p)$ (p 素数)证明即可. 考虑 G_k 是 $\mathbf{C}$ 之格集合 $\mathscr{R}$ 上的函数. 我们有

$$G_k(\Gamma)=\sum_{\gamma\in\Gamma}{}' 1/\gamma^{2k}\quad(见 § 2.3),$$

以及 $$T(p)G_k(\Gamma)=\sum_{(\Gamma:\Gamma')=p}\sum_{\gamma\in\Gamma'}{}' 1/\gamma^{2k}.$$

令 $\gamma\in\Gamma$. 如果 $\gamma\in p\Gamma$, 则 γ 属于在 Γ 中指标为 p 的 $(p+1)$ 个子格中的每一个. 它在 $T(p)G_k(\Gamma)$ 中的贡献是 $(p+1)/\gamma^{2k}$. 如果 $\gamma\in\Gamma-p\Gamma$, 则 γ 只属于指标 p 的一个子格, 它的贡献是 $1/\gamma^{2k}$. 因此

$$\begin{aligned}T(p)G_k(\Gamma)&=G_k(\Gamma)+p\sum_{\gamma\in p\Gamma}1/\gamma^{2k}\\&=G_k(\Gamma)+pG_k(p\Gamma)=(1+p^{1-2k})G_k(\Gamma).\end{aligned}$$

这就证明了 G_k(看作是 $\mathscr{R}$ 上的函数) 为 $T(p)$ 的本征函数, 而且本征值是 $1+p^{1-2k}$. 于是作为模形式, G_k 是 $T(p)$ 的本征函数, 而且本征值是 $p^{2k-1}(1+p^{1-2k})=\sigma_{2k-1}(p)$. § 4.2 中的公式(34)和(36)表明, 与 G_k 相结合的标准化本征函数是

$$(-1)^k\frac{B_k}{4k}+\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n.$$

这也表明 $T(n)$ 的本征值是 $\sigma_{2k-1}(n)$. 最后

$$\begin{aligned}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)/n^s&=\sum_{a,d\geq 1}a^{2k-1}/a^sd^s\\&=\Big(\sum_{d\geq 1}1/d^s\Big)\Big(\sum_{a\geq 1}1/a^{s+1-2k}\Big)\\&=\zeta(s)\zeta(s-2k+1).\end{aligned}$$

b) Δ 函数.

命题 14 Δ 函数是 $T(n)$ 的本征函数. 对应的本征值是 $\tau(n)$, 而标准化本征函数是

$$(2\pi)^{-12}\Delta=q\prod_{n=1}(1-q^n)^{24}=\sum_{n=1}^{\infty}\tau(n)q^n.$$

证 这是显然的, 因为权 12 的 cusp 型空间的维数是 1, 并且它在 $T(n)$ 作用下不变.

系 我们有

(52) $$\tau(nm)=\tau(n)\tau(m) \quad (\text{如果}(m,\ n)=1).$$

(53) $$\tau(p)\tau(p^n)=\tau(p^{n+1})+p^{11}\tau(p^{n-1}) \quad (p\ \text{素数},\ n\geqslant 1).$$

证 这从定理 7 的系 2 推出.

注 如果权 $2k$ 的 cusp 型空间 M_k^0 的维数是 1,则有类似结果. 这样的 k 为

$$k=6,\ 8,\ 9,\ 10,\ 11,\ 13.$$

基分别为 $\Delta,\ \Delta G_2,\ \Delta G_3,\ \Delta G_4,\ \Delta G_5$ 和 ΔG_7.

5.6. 补充

5.6.1. Petersson 内积

设 $f,\ g$ 是权 $2k(k>0)$ 的两个 cusp 型. 容易证明测度

$$\mu(f,\ g)=f(z)\overline{g(z)}y^{2k}dxdy/y^2 \quad (x=\mathrm{Re}(z),\ y=\mathrm{Im}(z))$$

是 G-不变的,并且在商空间 H/G 上这是有界测度. 令

(87) $$\langle f,\ g\rangle=\int_{H/G}\mu(f,\ g)=\int_D f(z)\overline{g(z)}y^{2k-2}dxdy,$$

我们得到 M_k^0 上一个 Hermite 内积, 它是正定非退化的. 可以验证

(88) $$\langle T(n)f,\ g\rangle=\langle f,\ T(n)g\rangle.$$

这表明 $T(n)$ 是关于 $\langle f,\ g\rangle$ 的 Hermite 算子. 由于 $T(n)$ 之间是彼此可交换的,一个熟知的命题可推出: 存在 M_k^0 的一组正交基, 使它们均是 $T(n)$ 的本征向量, 并且 $T(n)$ 的本征值都是实数.

5.6.2. 整性

设

$$M_k(\mathbf{Z})=\left\{\text{权 } 2k \text{ 模形式 } f=\sum_{n=0}^{\infty}c(n)q^n \,\middle|\, c(n)\text{是整数}\right\}.$$

可以证明存在 $M_k(\mathbf{Z})$ 的 $\mathbf{Z}$-基, 使它也是 M_k 的 $\mathbf{C}$-基. [更确切

地说，可以验证 $M_k(\mathbf{Z})$ 有如下的基（注意 $F=q\prod(1-q^n)^{24}$）：

k 为偶数时：$\{E_2^\alpha F^\beta \mid \alpha+3\beta=k/2,\ \alpha,\ \beta\in\mathbf{N}\}$，

k 为奇数时：$\left\{E_3E_2^\alpha F^\beta \mid \alpha+3\beta=\dfrac{k-3}{2},\ \alpha,\ \beta\in\mathbf{N}\right\}$.]

命题 12 表明 $M_k(\mathbf{Z})$ 是 $T(n)$ $(n\geqslant1)$ 作用下不变的．由此即得到结论：$T(n)$ 在 M_k 上作用的本征多项式是整系数的[注]．特别地，$T(n)$ 的本征值是代数整数（由 5.6.1 可知它们是"全实的"）．

5.6.3．Ramanujan-Petersson 猜想

设 $f=\sum_{n\geqslant1}c(n)q^n$，$c(1)=1$ 是权 $2k$ 的 cusp 型，并且是 $T(n)$ 的标准本征函数．令 $\Phi_{f,p}(T)=1-c(p)T+p^{2k-1}T^2$ (p 素数)是 § 5.4 公式(83)中定义的多项式．我们可以写

(89) $$\Phi_{f,p}(T)=(1-\alpha_pT)(1-\alpha'_pT),$$

其中

(90) $$\alpha_p+\alpha'_p=c(p),\qquad \alpha_p\alpha'_p=p^{2k-1}.$$

Petersson 猜想是：α_p 和 α'_p 是复共轭的．这也可以表示成

$$|\alpha_p|=|\alpha'_p|=p^{k-1/2},$$

或者 $$|c(p)|\leqslant 2p^{k-1/2},$$

或者 $$|c(n)|\leqslant n^{k-1/2}\sigma_0(n)\quad(\text{对一切 } n\geqslant1).$$

对于 $k=6$，这给出 Ramanujan 猜想：$|\tau(p)|\leqslant 2p^{11/2}$.

（这个猜想可以从有限域上代数流形的广义 Weil 猜想推出来，见 P. Deligne, Bourbaki 讨论班 1968/69, n°355.(*)）

[注] 我们指出，存在关于 $T(n)$ 的迹的显公式，见 M. Eichler 和 A. Selberg, Jour. Indian Math. Soc., 20, 1956.

(*) 关于有限域上代数流形的广义 Weil 猜想已被 P. Deligne 所证明，见前注所引文献．——译者注

§6. Theta 函 数

6.1. Poisson 公式

设 V 是 n 维实向量空间，具有不变测度 μ. 设 V' 是 V 的对偶空间. 令 f 为 V 上快降光滑函数 (见 L. Schwartz, Théorie des Distributions, 第七章 § 3). f 的 Fourier 变换 f' 定义为

$$f'(y)=\int_V e^{-2\pi i\langle x, y\rangle} f(x)\mu(x). \tag{91}$$

这是 V' 上的快降光滑函数.

现在设 Γ 是 V 的格 (见 § 2.2). 以 Γ' 表示 V' 中与 Γ 对偶的格，即

$$\Gamma'=\{y\in V' \mid \langle x, y\rangle\in\mathbf{Z}, \text{ 对每个 } x\in\Gamma\}.$$

不难验证 Γ' 可以等同于 Γ 之 $\mathbf{Z}$-对偶 (因此叫这样的术语).

命题 15 设 $v=\mu(V/\Gamma)$, 则有

$$\sum_{x\in\Gamma} f(x)=\frac{1}{v}\sum_{y\in\Gamma'} f'(y). \tag{92}$$

用 $v^{-1}\mu$ 代替 μ 之后，我们可设 $\mu(V/\Gamma)=1$. 取 Γ 的一组基 $e_1, \cdots, e_n$, 我们可以把 V 等同于 $\mathbf{R}^n$, 而 Γ 等同于 $\mathbf{Z}^n$, μ 为积测度 $dx_1\cdots dx_n$. 这时我们有 $V'=\mathbf{R}^n$, $\Gamma'=\mathbf{Z}^n$, 从而我们归结为古典的 Poisson 公式 (Schwartz, 同上，第七章公式 (7:5)).

6.2. 到二次型的应用

以下设 V 具有正定非退化双线性型 $x\cdot y$ (即 $x\neq 0$ 时 $x\cdot x>0$). 利用这个双线性型我们把 V' 等同于 V, 于是格 Γ' 变成 V 中的格. 我们有

$$y\in\Gamma'\Leftrightarrow x\cdot y\in\mathbf{Z}\quad(\text{对一切 } x\in\Gamma).$$

对于格 Γ，我们结合一个定义在 $\mathbf{R}_+^*$ 上的函数：

(93) $$\Theta_\Gamma(t)=\sum_{x\in\Gamma}e^{-\pi t x\cdot x}.$$

我们在 V 上选取不变测度 μ，使得若 $\varepsilon_1,\cdots,\varepsilon_n$ 是 V 的正交基，则由 ε_i 定义的单位立方体的体积是 1。于是格 Γ 的体积可以定义成 $v=\mu(V/\Gamma)$，见 § 6.1.

命题 16 我们有恒等式

(94) $$\Theta_\Gamma(t)=t^{-n/2}v^{-1}\Theta_{\Gamma'}(t^{-1}).$$

证 令 $f=e^{-\pi x\cdot x}$，这是 V 上快降光滑函数. f 的 Fourier 变换 f' 等于 f. 事实上，取 V 之一组正交基，并且用这组基将 V 等同于 $\mathbf{R}^n$. 则测度 μ 变成测度 $dx=dx_1\cdots dx_n$，而函数 f 是

$$f=e^{-\pi(x_1^2+\cdots+x_n^2)}.$$

于是我们归结为证明 $e^{-\pi x^2}$ 的 Fourier 变换是 $e^{-\pi x^2}$，而这一点是熟知的.

现在将命题 15 用于函数 f 和格 $t^{1/2}\Gamma$. 这个格的体积是 $t^{n/2}v$，而它的对偶是 $t^{-1/2}\Gamma'$，就给出我们要证的公式.

6.3. 矩阵解释

设 $e_1,\cdots,e_n$ 是 Γ 的一组基. 令 $a_{ij}=e_i\cdot e_j$. 则矩阵 $A=(a_{ij})$ 是非退化正定对称的. 如果 $x=\sum x_ie_i\in V$，则

$$x\cdot x=\sum a_{ij}x_i\cdot x_j.$$

函数 Θ_Γ 可以写成

(95) $$\Theta_\Gamma(t)=\sum_{x_i\in\mathbf{Z}}e^{-\pi t\sum a_{ij}x_ix_j}.$$

Γ 的体积为

(96) $$v=\det(A)^{1/2}.$$

这可以如下看出：设 $\varepsilon_1, \cdots, \varepsilon_n$ 是 V 的一组正交基，而令

$$\varepsilon=\varepsilon_1\wedge\cdots\wedge\varepsilon_n, \quad e=e_1\wedge\cdots\wedge e_n,$$

我们有 $e=\lambda\varepsilon$，其中 $|\lambda|=v$. 另一方面，$e\cdot e=\det(A)\varepsilon\cdot\varepsilon$. 比较之即得到 $v^2=\det(A)$.

令 $B=(b_{ij})=A^{-1}$，不难验证 (e_i) 之对偶基由下式给出：

$$e'_i=\sum b_{ij}e_j.$$

(e'_i) 形成 Γ' 的一组基，$B=(e'_i\cdot e'_j)$. 特别地，这证明了，如果 $v'=\mu(V/\Gamma')$，则 $vv'=1$.

6.4. 特殊情形

我们对于具有下述两个性质的 (V, Γ) 感兴趣：

(i) $\Gamma'=\Gamma$.

这意味着 $x, y\in\Gamma$ 时 $x\cdot y\in\mathbf{Z}$，并且型 $x\cdot y$ 定义了 Γ 到自身之上的同构. 用矩阵语言，这意味着矩阵 $A=(e_i\cdot e_j)$ 有整系数并且它的行列式等于1. 根据(96)式，后一条件等价于 $v=1$.

如果 $n=\dim V$，这个条件推出二次模 Γ 属于第五章 §1.1 定义的范畴 S_n. 反之，如果 $\Gamma\in S_n$ 是正定的并且令 $V=\Gamma\otimes\mathbf{R}$，则 (V, Γ) 满足(i).

(ii) 对于每个 $x\in\Gamma$ 均有 $x\cdot x\equiv 0 \pmod 2$.

这意味着 Γ 是第 II 类的(在第五章 §1.3.5 的意义下)，或者说矩阵 A 的对角元素 $e_i\cdot e_i$ 均是偶数.

我们在第五章已经给出过这种格 Γ 的一些例子.

6.5. Theta 函数

在本小节和下一小节中，我们假定 (V, Γ) 满足上一小节中的条件(i)和(ii).

设 $m\geqslant 0$ 为整数，以 $r_\Gamma(m)$ 表示集合

$$\{x\in\Gamma \mid x\cdot x=2m\}$$

的元素个数. 容易看出 $r_\Gamma(m)$ 为 m 的一个多项式所界(例如，一个粗糙的体积推导可以给出 $r_\Gamma(m)=O(m^{n/2})$). 这表明整系数级数

$$\sum_{m=0}^{\infty} r_\Gamma(m)q^m=1+r_\Gamma(1)q+\cdots$$

在 $|q|<1$ 中收敛. 于是可以在半平面 H 上定义函数 θ_Γ:

(97) $$\theta_\Gamma(z)=\sum_{m=0}^{\infty} r_\Gamma(m)q^m \quad (q=e^{2\pi iz}).$$

我们有

(98) $$\theta_\Gamma(z)=\sum_{x\in\Gamma} q^{(x\cdot x)/2}=\sum_{x\in\Gamma} e^{\pi iz(x\cdot x)}.$$

函数 $\theta_\Gamma(z)$ 叫作二次模 Γ 的 theta 函数. 它在 H 上全纯.

定理 8 (a) V 的维数 n 是 8 的倍数.

(b) 函数 θ_Γ 是权 $n/2$ 的模形式.

证 (a) 已经证过(第五章 § 2.1 定理 2 的系 2).

我们证明恒等式

(99) $$\theta_\Gamma(-1/z)=(iz)^{n/2}\theta_\Gamma(z).$$

因为两边对于 z 都是解析的，只需对 $z=it(t>0)$ 证明此公式. 我们有

$$\theta_\Gamma(it)=\sum_{x\in\Gamma} e^{-\pi t(x\cdot x)}=\Theta_\Gamma(t).$$

类似地，$\theta_\Gamma(-1/it)=\Theta_\Gamma(t^{-1})$. 于是在公式 (94) 中考虑到 $v=1$ 和 $\Gamma=\Gamma'$ 即给出公式(99).

因为 $8|n$，我们可以把(99)式重写为

(100) $$\theta_\Gamma(-1/z)=z^{n/2}\theta_\Gamma(z).$$

这就表明 θ_Γ 是权 $n/2$ 的模型.

[我们简要地给出(a)的另一个证明. 假设 $8\nmid n$，必要时

用 $\Gamma\oplus\Gamma$ 或者 $\Gamma\oplus\Gamma\oplus\Gamma\oplus\Gamma$ 代替 Γ，可设 $n\equiv4\pmod 8$. 这时公式(99)可以写成

$$\theta_\Gamma(-1/z)=(-1)^{n/4}z^{n/2}\theta_\Gamma(z)=-z^{n/2}\theta_\Gamma(z).$$

如果令 $\omega(z)=\theta_\Gamma(z)dz^{n/4}$，我们看到微分型 ω 在 S: $z\mapsto -1/z$ 之下变成 $-\omega$. 由于 ω 在 T: $z\mapsto z+1$ 之下不变，因此 ST 将 ω 变为 $-\omega$，而这是不可能的，因为 $(ST)^3=1$.]

系 1 存在着权 $n/2$ 的 cusp 型 f_Γ，使得

(101) $$\theta_\Gamma=E_k+f_\Gamma,\quad 其中\ k=n/4.$$

证 由于 $\theta_\Gamma(\infty)=1$，从而 $\theta_\Gamma-E_k$ 是 cusp 型，由此即得结论.

系 2 我们有 $r_\Gamma(m)=\dfrac{4k}{B_k}\sigma_{2k-1}(m)+O(m^k)$，$k=n/4$.

证 这从系 1，公式(34)和定理 5 推出.

注 "误差项" f_Γ 一般不为零. 但是 Siegel 证明了 f_Γ 的加权平均是零. 更确切地说，以 C_n 表示满足条件 (i) 和 (ii) 的格同构类集合，以 g_Γ 表示 $\Gamma\in C_n$ 的自同构群的阶数(见第五章 § 3.3)，则有

(102) $$\sum_{\Gamma\in C_n}\frac{1}{g_\Gamma}\cdot f_\Gamma=0,$$

或者等价地，

(103) $$\sum_{\Gamma\in C_n}\frac{1}{g_\Gamma}\theta_\Gamma=M_nE_k,\quad 其中\ M_n=\sum_{\Gamma\in C_n}\frac{1}{g_\Gamma}.$$

注意这也等价于说，θ_Γ 的加权平均是诸 $T(n)$ 的本征函数.

公式(102)和(103)的证明见 C. L. Siegel 全集 n°20.

6.6. 例子

i) $n=8$ 情形.

权 $n/2=4$ 的每个 cusp 型均为零，于是由定理 8 的系 1

可知 $\theta_\Gamma=E_2$，换句话说，

(104) $\quad r_\Gamma(m)=240\sigma_3(m)\quad$ (对于每个整数 $m\geqslant 1$).

这可用于第五章 § 1.4.3 中构作的格 Γ_8(注意这个格是 C_8 中唯一的元素).

ii) $n=16$ 情形.

我们有(理由同上)

(105) $$\theta_\Gamma=E_4=1+480\sum_{m=1}^{\infty}\sigma_7(m)q^m,$$

这里可取 $\Gamma=\Gamma_8\oplus\Gamma_8$ 或者 $\Gamma=\Gamma_{16}$(记号见第五章 § 1.4.3). 这两个格虽然不同构，但是有同样的 zeta 函数，即它们表示每个整数的次数是一样的.

注意附着于格 $\Gamma_8\oplus\Gamma_8$ 的函数 θ 是 Γ_8 的函数 θ 的平方. 因此我们发现一个恒等式:

$$\left(1+240\sum_{m=1}^{\infty}\sigma_3(m)q^m\right)^2=1+480\sum_{m=1}^{\infty}\sigma_7(m)q^m.$$

iii) $n=24$ 情形.

权 12 的模形式空间是 2 维的. 它的基可取如下的两个函数:

$$E_6=1+\frac{65520}{691}\sum_{m=1}^{\infty}\sigma_{11}(m)q^m,$$

$$F=(2\pi)^{-12}\Delta=q\prod_{m=1}^{\infty}(1-q^m)^{24}=\sum_{m=1}^{\infty}\tau(m)q^m.$$

于是，与格 Γ 相结合的 theta 函数可以写成

(106) $$\theta_\Gamma=E_6+c_\Gamma F\quad(c_\Gamma\in\mathbf{Q}).$$

我们有

(107) $$r_\Gamma(m)=\frac{65520}{691}\sigma_{11}(m)+c_\Gamma\tau(m)\quad(m\geqslant 1).$$

取 $m=1$ 即决定系数 c_Γ:

$$c_\Gamma = r_\Gamma(1) - \frac{65520}{691}. \tag{108}$$

由于 65520/691 不是整数，从而 $c_\Gamma \neq 0$.

【例】 a) J. Leech 所构作的格（Canad. J. Math., 16, 1964）是 $r_\Gamma(1)=0$, 于是

$$c_\Gamma = -\frac{65520}{691} = -2^4 \times 3^2 \times 5 \times 7 \times 13/691.$$

b) 对于 $\Gamma = \Gamma_8 \oplus \Gamma_8 \oplus \Gamma_8$, 我们有 $r_\Gamma(1) = 3 \times 240$, 于是

$$c_\Gamma = \frac{432000}{691} = 2^7 \times 3^3 \times 5^3/691.$$

c) 对于 $\Gamma = \Gamma_{24}$, 我们有 $r_\Gamma(1) = 2 \times 24 \times 23$, 于是

$$c_\Gamma = \frac{697344}{691} = 2^{10} \times 3 \times 227/691.$$

6.7. 补充

由于我们只考虑全模群 $G = \mathrm{PSL}_2(\mathbf{Z})$, 使我们只限于研究 § 6.4 中具有很强条件的格. 特别地，我们不能处理最自然的情形，即二次型

$$x_1^2 + \cdots + x_n^2.$$

这个二次型满足条件(i)，但是不满足条件(ii). 它所对应的 theta 函数对于 G 的由 S 和 T^2 生成的子群是"权 $n/2$ 的模形式"(注意 $n/2$ 不一定是整数). G 的这个子群对于 G 的指标为 3, 它的基本区域有两个"cusp", 对应这两个"cusp"有两种类型的"Eisenstein 级数". 使用这些 Eisenstein 级数，我们得到把一个整数表为 n 个平方之和的表现个数公式，详见文献目录中所引的书和文章.

文　献

一些经典著作

C. F. Gauss—Disquisitiones arithmeticae, 1801, Werke, Bd. I.(英译本: Yale Univ. Press; 法译本: Blanchard.)

C. Jacobi—Fundamenta nova theoriae functionum ellipticarum, 1829, Gesammelte Werke, Bd. I., pp. 49～239.

G. Lejeune Dirichlet—Démonstration d'un théorème sur la progression arithmétique, 1834, Werke, Bd. I. p. 307.

G. Eisenstein—Mathematische Abhandlungen, Berlin, 1847 (1967 年再版: Georg Olms Verlag., Hildescheim).

B. Riemann—Gesammelte mathematische Werke, Teubner, 1892 (英译本: Dover; 部分法译本: Gauthier-Villars, 1898).

D. Hilbert—Die Theorie der algebraischer Zahlkörper, Gesam. Abh., Bd. I. pp. 63～363(法译本: Ann. Fac. Sci. Toulouse, 1909 和 1910).

H. Minkowski—Gesammelte Abhandlungen, Teubner, 1911.

A. Hurwitz—Mathematische Werke, Birkhäuser, Verlag, 1932.

E. Hecke—Mathematische Werke, Göttingen, 1959.

C. L. Siegel—Gesammelte Abhandlungen, Springer-Verlag, 1966.

数域和局部域

E. Hecke—Algebraische Zahlen, Leipzig, 1923.

Z. I. Borevich 和 I. R. Shafarevich—Number Theory (译自俄文), Academic Press, 1966.(有法译本和德译本).

M. Eichler—Einführung in die Theorie der algebraischen Zahlen und Funktionen, Birkhauser Verlag, 1963 (英译本: Academic Press, 1966).

J-P. Serre—Corps Locaux, Hermann, 1962.

P. Samuel—Théorie algébrique des nombres, Hermann, 1967.

E. Artin 和 J. Tate—Class Field Theory, Benjamin, 1968.

J. Cassels 和 A. Fröhlich (编)—Algebraic Number Theory, Academic Press,

1967.

A. Weil—Basic Number Theory, Springer-Verlag, 1967.

S. Lang—Algebraic Number Theory, Addison-Wesley, 1970.

(后四个著作包含"类域论"内容.)

二次型

a) 一般理论, Witt 定理

E. Witt—Theorie der quadratischen Formen in beliebigen Körpern, J. Crelle, 176, 1937, pp. 31～44.

N. Bourbaki—Algèbre, chap. IX, Hermann, 1959.

E. Artin—Geometric Algebra, Interscience Publ., 1957 (法译本: Gauthier-Villars, 1962).

b) 算术性质

B. Jones—The arithmetic theory of quadratic forms, Carus Mon., n°10, John Wiley and Sons, 1950.

M. Eichler—Quadratische Formen und orthogonale Gruppen, Springer-Verlag, 1952.

G. L. Watson—Integral quadratic forms, Cambridge Tracts, n°51, Cambridge. 1960.

O. T. O' Meara—Introduction to quadratic forms, Springer-Verlag, 1963.

c) 判别式为 ±1 的整二次型

E. Witt—Eine Identität zwischen Modulformen zweiten Grades, Abh. math. Sem. Univ. Hamburg, 14, 1941, pp. 323～337.

M. Kneser—Klassenzahlen definiter quadratischer Formen, Arch. der Math. 8, 1957, pp. 241～250.

J. Milnor—On simply connected manifolds, Symp. Mexico, 1958, pp. 122～128.

J. Milnor—A procedure for killing homotopy groups of differentiable manifolds, Symp. Amer. Math. Soc., n°3, 1961, pp. 39～55.

Dirichlet 定理, zeta 函数和 L-函数

J. Hadamard—Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques, 1896, Oeuvres, CNRS, t. 1, pp. 189～210.

E. Landau—Handbuch der Lehre von der Verteilung der Primzahlen, Teubner, 1909.

A. Selberg—An elementary proof of the prime number theorem for arithmetic progressions, Canad. J. Math., 2, 1950, pp. 66～78.

K. Prachar—Primzahlverteilung, Springer-Verlag, 1957.

H. Davenport—Multiplicative number theory, Markham, Chicago, 1968.

K. Chandrasekharan—Introduction to analytic number theory, Springer-Verlag, 1968.

A. Blanchard—Initiation à la théorie analytique des nombres premiers, Dunod, 1969.

模函数

F. Klein—Vorlesungen über die Theorie der elliptischen Modulfunktionen, Leipzig, 1890.

S. Ramanujan—On certain arithmetical functions, Trans. Cambridge Phil. Soc., 22, 1916, pp. 159～184.

G. Hardy—Ramanujan, Cambridge Univ. Press, 1940.

R. Godement—Travaux de Hecke, Sém. Bourbaki, 1952～53, exposés 74, 80.

R. C. Gunning—Lectures on modular forms (notes by A. Brumer), Ann. of Math. Studies, Princeton, 1962.

A. Borel et al.—Seminar on complex multiplication, Lecture Notes in Maths., n°21, Springer-Verlag, 1966.

A. Weil—Sur la formule de Siegel dans la théorie des groups classiques, Acta Math., 113, 1965, pp. 1～87.

A. Ogg—Modular forms and Dirichlet series, Benjamin, 1969.

G. Shimura—Introduction to the arithmetic theory of automorphic functions, Tokyo-Princeton, 1971.

(还参见上面所引的 Hecke 和 Siegel 著作.)

符 号 索 引

期 阳

定 义 索 引